CONNECTING THE DOTS.
INTELLIGENCE AND LAW ENFORCEMENT SINCE 9/11

by

Mary Margaret Stalcup

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Joint Doctor of Philosophy
with University of California, San Francisco

in

Medical Anthropology

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Paul Rabinow, Chair
Professor Dorothy Porter
Professor Candace Slater

Fall 2009

The dissertation of Mary Margaret Stalcup, titled Connecting the Dots. Intelligence and Law Enforcement since 9/11, is approved:

Chair: ____ Date _____________

____ Date _____________

____ Date _____________

University of California, Berkeley

Connecting the Dots. Intelligence and Law Enforcement since 9/11

by Mary Margaret Stalcup

Abstract

Connecting the Dots. Intelligence and Law Enforcement since 9/11

by

Mary Margaret Stalcup

Joint Doctor of Philosophy in Medical Anthropology
with University of California, San Francisco

University of California, Berkeley

Professor Paul Rabinow, Chair

This work examines how the conceptualization of knowledge as both problem and solution reconfigured intelligence and law enforcement after 9/11. The idea was that more information should be collected, and better analyzed. If the intelligence that resulted was shared, then terrorists could be identified, their acts predicted, and ultimately prevented. Law enforcement entered into this scenario in the United States, and internationally. “Policing terrorism” refers to the engagement of state and local law enforcement in intelligence, as well as approaching terrorism as a legal crime, in addition to or as opposed to an act of war. Two venues are explored: fusion centers in the United States and the international organization of police, Interpol. The configuration can be thought of schematically as operating through the set of law, discipline and security. Intelligence is predominantly a security approach. It modulates that within its purview, wielding the techniques and technologies that are here discussed.

The dissertation is divided into two sections: Intelligence and Policing Terrorism. In the first, intelligence is taken up as a term, and its changes in referent and concept are examined. The Preface and Chapter One present a general introduction to the contemporary situation and intelligence, via Sherman Kent, as knowledge, organization and activities. Chapter Two traces the development of intelligence in the United States as a craft and profession. Chapter Three discusses some of the issues involving the intersection of intelligence and policy, and how those manifested in the aftermath of 9/11 and the lead up to the 2003 invasion of Iraq. The second section examines the turn to policing terrorism, beginning, in Chapter Four, with how Interpol has dealt with bioterrorism, and an examination of the shifting conceptualization of biological threats in international law. Moving from threats to their consequences, Chapter Five takes up the concept of an event in order to analyze the common comparison of Pearl Harbor and 9/11. Chapters Six and Seven turn to fieldwork done in the United States, with an examination of the suspicious activity reporting system and law enforcement’s inclusion in the Information Sharing Environment, focusing on fusion centers and data mining.

For Dennis Irwin 1951-2008

“All Ears, All The Time”

Connecting the Dots.

Intelligence and Law Enforcement since 9/11

PART I. Intelligence

PART II. Policing Terrorism

Acknowledgements

It is a pleasure to acknowledge the intellectual exchanges, quotidian support and friendships that helped me in the process of researching and writing this dissertation.

At home, my parents, Alex and Janice Stalcup, and my brothers, especially Luke Stalcup, welcomed my anthropology cohort into their house many times, and supported me with meals, transportation and encouragement. They also actively worked on developing and implementing this project; it would not have been possible without them.

At the fusion center, I will leave people unnamed, but they know who they are and have my gratitude for trusting me to do this research, accepting me with an open mind and without restrictions on what I would produce, engaging in many hours of conversation, and taking me to the DEA gym.

In France, my thanks to the people at Interpol who assisted me, and to the people who made a difference in my life in Lyon: members of Grupo Capoeira de Angola Cabula, Sophie Chiha, Xavier Dagany, Violaine L'hotellerie, Sophie Pailhes, Brian Rudkin and his family, and Scott Spence.

In Berkeley and San Francisco, I would especially like to thank the participants of the labinar; members of the Anthropology of the Contemporary Research Collaboratory; the staff at Espresso Roma, the UC Berkeley RSF, Interlibrary Services, in particular Shannon Monroe, and the anthropology department, in particular Ned Garrett; Professors Lawrence Cohen and Nancy Scheper-Hughes, who first gave me a chance; Professors Bill Hanks, Rosemary Joyce, Stefania Pandolfo, and Sharon Kaufman for courses and departmental support; members of my cohort, notably Monica Eppinger for her explanations of law, Carlo Caduff, and Nicholas Langlitz; Misha MacLaird for copyediting and company while writing; Ryan Sayre, for his critique of several chapter drafts; Roger Brent, for his sustained interest; the members of my committee, Professors Dorothy Porter and Candace Slater, and my advisor Paul Rabinow, for both allowing and demanding intellectual honesty, and for his unwavering care.

List of Acronyms

ACLU: American Civil Liberties Union

BW: Biological weapons

BWC: Biological Weapons Convention (Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological [Biological] and Toxin Weapons and on Their Destruction)

CATIC: California Anti-Terrorism Information Center

CDC: Center for Disease Control

CHHP: Center for Health Hazards Preparedness

CHP: California Highway Patrol

CIA: Central Intelligence Agency

CJIS: Criminal Justice Information System

COI: (Office of) Coordinator of Information

CTR: Cash Transaction Report

DA: District Attorney

DARPA: Defense Advanced Research Projects Agency

DEA: Drug Enforcement Administration

DHS: Department of Homeland Security

DMV: Department of Motor Vehicles

DOD: Department of Defense

DOJ: Department of Justice

EPIC: El Paso Intelligence Center

FBI: Federal Bureau of Investigation

FBI–NCIC: Federal Bureau of Investigation National Crime Information Center

FEMA: Federal Emergency Management Agency

FI: Field Information

FISA: Foreign Intelligence Surveillance Act

HE: High explosives

HIDTA: High-Intensity Drug Trafficking Area

HIFCA: High-Intensity Financial Crimes Area

IC: Intelligence Communities

IDW: Investigative Data Warehouse

ILP: Intelligence-led policing

Interpol: International Criminal Police Organization

IRTPA: Intelligence Reform and Terrorism Prevention Act

IRS: Internal Revenue Service

ISE-SAR: (National) Information Sharing Environment Suspicious Activity Reporting (Initiative)

JIS: Jamiyyat Ul-Islam Is-Saheeh

JTTF: Joint Terrorism Task Force

MDR-TB: Multiple-drug-resistant tuberculosis

NIE: National Intelligence Estimate

NLETS: National Law Enforcement Telecommunications System

NSSM: National Security Study Memorandum

OSP: Office of Special Plans (Pentagon)

OSS: Office of Strategic Services

OUSDP: Office of the Under Secretary of Defense for Policy

POP: Problem-Oriented Policing

POST: Police Officer Standards and Training

PSAC: President’s Science Advisory Committee

RTTAC: Regional Terrorism Threat Assessment Center

SAR: Suspicious Activity Report

TLO: Terrorism liaison officer

VERTIC: Verification Research, Training and Information Centre

WMD: Weapon(s) of Mass Destruction

WMDC: Weapons of Mass Destruction Commission

WSIN: Western States Information Network

XDR-TB: Extensively drug-resistant tuberculosis

PREFACE

Knowledge as Problem and Solution

"Connecting the dots" as a metaphor for intelligence analysis became popular with the 9/11 Commission Report. What is the message in that child's drawing game? Information is so many scattered, random dots. If joined together they will suddenly present an image of reality.

From dots to picture corresponds to the transformation of information into intelligence. Analysis is equated with child's play, but not unproblematically. This is a limited and stifling game. The dots are simply lying there on the page. There is one, correct way to connect them. Ignored are the practical and ethical challenges that collection really presents, and the potential for mutability of the pictures. Intelligence, an epistemologically unique and ultimately shadowy kind of knowledge, is equated with neatly linked pieces of data. The parallel is reductive but powerful, a rhetorical strategy, like the "war on terror" before it, which vigorously reshaped the intelligence assemblage after 9/11 in the United States and beyond.

The reconfiguration of intelligence was guided by a conceptualization of the problem as one of knowledge. Rectifying knowledge then became the solution. This circle was rendered concrete as the need for more and better intelligence. The scenario was little questioned: if those in government got more information, if they analyzed it better, if they shared the knowledge, then they could prevent terrorism. The following study traces how this logic led in two directions. One tangible outcome of the "knowledge solution" was a move to integrate state and local police into the foundation of a new intelligence architecture. Yet too much information is also a problem. The mass digitalization of life—captured and held in databases—presented too many dots. Techniques of data mining developed to process, filter and connect their otherwise overwhelming proliferation.

The "knowledge solution" is linked to the challenge of prediction, and technological ambitions. A distinctive diagram of power has developed,[1] one concerned with collecting and connecting dots into a "seamless web" of information. A web, however, is an intricate assemblage of *many* seams, threads and their conjunctions. Seamlessness is rather an ideal of circulation, without hitches or blockages. The technical web of intelligence is designed to discern threats and, by allowing decisions to be made, turn them into risks. The configuration can be schematically conceptualized, following Michel Foucault, as operating through the set of law, discipline and security. For analytical purposes, each is a distinctive and normative rationality. Security marshals legal prohibitions and disciplinary dictates to deal with unpredictable, unpreventable micro events, from suspicious behaviors to crimes. These are yoked into service as signs that point to truly catastrophic events, in order to avert them. Intelligence is predominantly a security approach. It modulates rather than strictly controls that within its purview, wielding the techniques and technologies that will be discussed in the following pages: ways of defining threats and

[1] Stephen J. Collier et al., "Concept Work: "Vital"," in *Concept Work*, Anthropology of the Contemporary Research Collaboratory (2009).

training officers to recognize them, standardizing behaviors, the creation of networks of surveillance, data analysis, and different types of data-mining.

As a term—a word and its referent—intelligence refers to 1) a historically developed practice that produces 2) a specific and definable kind of knowledge. This is 3) a target of intervention because of perceived inadequacies, and 4) a technology of a larger security apparatus.

In 2005, "national intelligence" was presented in a US government strategy document. The quotation marks were in the original. The writers wanted to signal a new concept, an integration of foreign and domestic intelligence that would exploit “risk while accepting the impossibility of eliminating it."[2] The strategy, which would mature into, among other things, the Information Sharing Environment, drew its legal authority from the previous year’s Intelligence Reform and Terrorism Prevention Act.[3] National intelligence, the Act mandated, would be explicitly oriented towards the future. There would be an institutional shift to a “preventative counterterrorism posture.” The goal was not simply to make it so that an attack of the magnitude of 9/11 could be detected and prevented, but to create an environment such that by default it *would* be. The dictum of conflict, that the defender must thwart all attempts, but the attacker need succeed only once, would be subverted. Attacks, or at least their preparations, would be taken from one side of the equation and put on the other. They would be enlisted as aids to grand scale prevention.

This vision took time to coalesce. “To one single set of difficulties, several responses can be made. And most of the time different responses actually are proposed.”[4] The elements that came together were less the result of unified interpretation or planning than a shared problematization. 9/11 introduced uncertainty across the spectrum of leaders and citizens, intelligence and law enforcement, federal and local government, the United States and the international community. The event’s formulation into a narrative with causes and consequences created the conditions of possibility for responses, “in their diversity and sometimes in spite of their contradictions.”[5] The following work deals with a heterogeneous group of these that can be glossed as “policing terrorism.” Some took root, adapted and flourished; others still struggle or have withered away.

Policing terrorism refers to the engagement of state and local law enforcement in intelligence, in order to “collect the dots” via surveillance and investigations. 9/11 effectively brought home global terrorism to the United States. The previous divide between foreign and domestic intelligence was viewed as a mistake. Police had long dealt with domestic extremism, but now they needed to add national security to their law and order duties. The US Director of National Intelligence made this clear: “The unique contribution made by men and women on the ground is vital to US national security… State and local partners should no longer be treated as only first responders; they are also the first lines of prevention.”[6]

[2] "National Intelligence Strategy of the United States of America," (Office of the Director of National Intelligence, 2005).

[3] *Intelligence Reform and Terrorism Prevention Act of 2004*, PL 108–458, 108th Congress (17 December 2004).

[4] Michel Foucault, "Polemics, Politics and Problematizations," in *Aesthetics, Method and Epistemology*, ed. James D Faubion (New York: New Press, 1998).

[5] Ibid.

[6] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs*, no. July/August (2007).

This dissertation explores two venues for policing terrorism: fusion centers and Interpol. Fusion centers, one of which I interned in from 2006 through 2007, are physical nodes in the intelligence and preparedness network developed as part of the Information Sharing Environment Initiative. Interpol, where I also interned, is the International Criminal Police Organization. This is rather different than “international police,” although they are often referred to that way. They do not enforce international laws, but serve as an information exchange for police to better enforce the laws in their own countries. Policing terrorism also encompasses the idea of approaching terrorism as a legal crime, in addition to or as opposed to an act of war. The use of the category of crime, more prevalent, established and disseminated than terrorism, moves towards a rejection of Islamic jihadists as the orienting enemy trope but also expands the range of ideological causes that are included, and thereby the need for and reach of counterterrorism actions. This expansion was what brought law enforcement and intelligence to my attention and how they became, partly by chance, the subject of my fieldwork.

My original focus was on the “war on drugs,” in the United States and Latin America. Narcotics officers were my incommensurable anthropological Other. I imagined three field sites, and made provisional trips to Brazil and Colombia, countries where I had spent time and in which I had contacts. In 2005, I began interviewing on the US side and arranged an internship with a counternarcotics group in California. When I began in counternarcotics in fall of 2006, joining an entering group of criminal intelligence analysts, I realized that something was in the process of happening. Human and financial resources were shifting from drugs to terrorism, and the motion was clearly a small part of a larger change. State, local and federal law enforcement agencies, single-issue task forces, and first responders were being gathered together in one of the then-new fusion centers that now populate almost every US state. Thus it was by chance that I found myself at the heart of counterterrorism efforts in a fusion center, but quite on purpose that I elected to follow this motion.

9/11 instigated, among other things, a multi-agency, interdisciplinary scramble for metaphors, analogies and tropes. Law enforcement was to be the new frontline in the domestic war on terror, the eyes and ears of the intelligence community, the foundation of the new intelligence architecture.[7] Police were no longer only first responders, but also first preventers. It was in order to see how far this shift went that, after finishing my internship at the fusion center, I went to Interpol, in Lyon, France. My internship there was in the Bioterrorism project, another intersection of law enforcement and counterterrorism efforts. My work was far removed from the on-the-ground counterterrorism of the fusion center. The project had two distinct thrusts. One provided trainings at a world regional level on how to deal with bioterrorism incidents. The other, where I worked, focused on implementation of the United Nations’ resolutions against the proliferation of biological weapons and potential bioterrorist acts.

Frank, the deputy director of the fusion center where I interned and a figure who will reappear in the following pages, told me that intelligence could be used to identify a pattern of behaviors that in turn could be used to identify a potential terrorist. Or from an identified person, one could trace outward to find a plan for terrorism. This is the point, he said.

Information—data and information—that has been analyzed becomes intelligence.

[7] Marilyn Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," ed. Department of Justice (Bureau of Justice Assistance, 2005), 4.

> The intelligence points in a particular direction. That direction is then shared back with the people who gather the bits and pieces of information, with some options or actions, which produces more data and information, which is fed right back into the system to be analyzed and reassessed.

In the face of the failure of 9/11, creating a system to gather, preserve and share information was logical. Some fervently believe, and others equally as fervently deny, that there are terrorism indicators in the chaos of daily life that can be spotted. In practical terms, this means a domestic system of intelligence, and a global information exchange (as Interpol desired to provide). Historically, though, similar concessions to the needs of security and increases in power have led to abuse. This is a study of what a preventative counterterrorism posture means in the register of daily practices. In what situations, and how, does a police officer discern danger, crime, and terrorism on an innocuous street, turn these into reports, and send them to the right place? In the register of the political, what has happened to set this system in place and how has it worked?

For the other deputy director of the fusion center, Jerome—another who will reappear in the following chapters—using all resources was due diligence.

> They always say that hindsight is 20/20 and it's nice to say what people should have done. These guys just learning how to fly planes and not land them, it was a problem. Now it looks silly, but there are things going on right now with incidents that are tied together, if we hadn't seen them ahead of time, we wouldn't know who to focus on. And they are silly things, which seem silly now, similar to that. But we are going now, you know, "this is awfully suspicious behavior, we need to track these people."

As a result, street cops are trained to notice, document and share potentially terrorism-related information that they come across on their beats. I studied how local law enforcement was being trained to serve as the most micro level of information-feed for domestic counter terrorism.

Yet, intelligence agencies and law enforcement have different missions. The purpose of an intelligence agency is to gather information. The means can be justified by the ends. The purpose of law enforcement is to produce "law and order," by its deterrent presence and the punishment meted out to those who break the law. In the criminal system, means must follow strict protocol or the ends will not be met. A concern in policing terrorism, as in related aspects of the Patriot Act and the transformation of law enforcement, is that using the police in an intelligence capacity will compromise their relationship to the law, and thereby corrupt their practice. Scenarios of concern include domestic surveillance, and investigations in situations that could not be justified for regular criminal pursuit, but have been justified for terrorist pursuit.

Returning to intelligence, the ways that humans construct and authorize knowledge is one of anthropology's oldest and most enduring topics. These inquiries share the question, what is knowledge and how can something can be known? As anthropology, they focus this philosophical query on the particular of both a time and a place. In the case of this dissertation, the anthropological goal is to offer substantive information about, reflection on, and insight into the "what, how and why" of a contingent present in the United States, and the indefinite realm of activity of international organizations, as I found it at Interpol. The history put together here is part of an iterative process to, in John Dewey's words, "discover and formulate the conditions which describe the problem at hand."[8] This account of some of the past and present history of intelligence, as a practice (craft, policy tool, discipline, science) is a quite literal examination of reasoning and rationalities, part of a project to anthropologize the west.[9] Public and academic discourses about the rapprochement of national security intelligence and criminal intelligence, and the role of the human sciences in national security are often curiously ahistorical, and a genealogical presentation of the pertinent histories mentioned above that will be developed.

The dissertation is divided into two sections, **Intelligence** and **Policing Terrorism**. The first examines intelligence as a term, and its changes in referent and concept. Chapter One presents a general introduction to the contemporary situation and then focuses on intelligence as, classically via Sherman Kent, knowledge, organization and activities. Chapter Two traces the development of intelligence in the United States as a craft and profession. Chapter Three discusses some of the issues involving the intersection of intelligence and policy, and how those manifested in the aftermath of 9/11 and the lead up to the 2003 invasion of Iraq.

The second section examines the turn to policing terrorism. The US rhetorically framed its anti- and counterterrorism initiative after 9/11 as *war*, a term that entrenched the physical space of the nation as a battleground, and justified a prolonged state of exception. The inclusion of native soil and the conceptualization of permanent threat made it simultaneously paradoxical and clearly logical to put law enforcement into the fight. However, the trope of war was gradually replaced with alternative approaches, one of which is "policing terrorism," brought into being with a series of directives and laws that refocused the efforts of state and local law enforcement.[10]

Part II: Policing Terrorism begins with Chapter Four's examination of Interpol and bioterrorism, through the shifting conceptualization of biological threats in international law. In other historical situations, threats were understood quite differently, and different responses were formulated. The chapter looks at three international accords on biological weapons and describes for each what threat is being addressed, the object of protection, and techniques proposed for intervention. Moving from threats to their consequences, Chapter Five takes up the concept of an event in order to analyze the common comparison of Pearl Harbor and 9/11. Pearl Harbor in its time was a scandal and the subject of nine congressional investigations. 9/11 has had only one. Many of the strategies described in this dissertation can be ascribed to the interpretation of 9/11 as intelligence failure, which is turn stems, at least partly, from the stabilization of this view by the 9/11 Committee. This postulation greatly impacted the development of the "war on terror" and how it should be fought. Chapters Six and Seven turn to the rest of my fieldwork, with an examination of the suspicious activity reporting system and law enforcement's inclusion in the Information Sharing Environment, focusing on fusion centers and data mining.

[8] John Dewey, Logic: The Theory of Inquiry, vol. 12, The Later Works, 1925-38 (New York, NY: Carbondale: Southern Illinois Press, 1991), 345-46 quoted in Paul Rabinow, *Marking Time: On the Anthropology of the Contemporary* (Princeton: Princeton University Press, 2008), 9.

[9] Paul Rabinow, Essays on the Anthropology of Reason (Princeton, N.J.: Princeton University Press, 1996).

[10] The FBI is a branch of law enforcement and is responsible for countering domestic terrorism. While it is also shifting, roughly from a focus on investigations of terrorist attempts to preventative investigations, the focus here is on the changes occurring state and local law enforcement.

Chapter One. Introductions

Jerome greets everyone with a wide smile. He is possessed of unflappable good humor and energy. "Early on in life," he recounted, "I decided I wanted to get into law enforcement. I grew up in a pretty impoverished area, lot of violence, lot of murders. There was a lot of seeing that growing up. I wanted to do something." He started working vice in the California Department of Alcoholic Beverage Control, and then went to a major crimes task force with the Bureau of Narcotic Enforcement before moving to methamphetamine investigation for the state's Department of Justice. Midmorning, September 11, 2001, he received a telephone call telling him he was being transferred to counterterrorism. "You got the call on the day?" I asked.

> They basically moved me and back-filled my old spot. I got transferred—I got a call on 9/11 saying, "you're being transferred to a new unit." I wasn't even in town, I was in, where the hell was I? I was in some range, I was actually at firearms instruction training… I don't remember the exact spot, but I was in some training in Northern California when they called me, and said "you're being transferred. We don't know what we're going to call it, but you're being transferred to a new unit." I said, "Okay, whatever we need to do." From there, there was an opening for a Criminal Intelligence Bureau Commander, that's how I came here.

Jerome was not alone; career trajectories from law enforcement to the sciences took a sharp turn that day, as the reallocation of personnel and funding to counterterrorism began. At once, the attacks were grasped as an event, ushering in a new era. Equally, if secondarily for most, they revealed that there was an existing problem. The terrorists were part of a bigger and organized group. They had lived in the United States and had common American lives before committing the attacks. These revelations and the challenges they presented to previous ideas about terrorism were to organize much of the response.

Jerome continued:

> I went over to working the California Anti-Terrorism Information Center Task Force, CATIC was what they originally called us. So the CATIC task forces, our mission was to go out and work on these cases. Basically—and this was a big part—the state of California did not trust the federal government. They felt that there was such a lapse that created September 11th that we needed to do our own project and track down these terrorists. And basically we got sent out, no real training on intelligence at the time, just "go out there and find terrorists." What do we do with them after we find them? "We'll figure that out later."

Priorities, usually defined in government by an unending political dance between constituencies, were provided instead by a shared sense of threat and urgency. Organization is something that can be detected. It requires communication, transportation, and funding. These leave traces. The common American life, and even more so the criminal one, is now digitally documented, archived and analyzed. If these signs are among us, they can be discerned. How and whom to watch, and who should do the watching?

The director of the fusion center where I did fieldwork, who was a thirty-year local narcotics veteran, explained the problem that he was attempting to solve.

> There are a lot of cops in America. County and municipal and state and private cops, 750- to 800,000 of them, and we thought—well, we never, I guess, felt like we were engaged in the world of international terrorism. You know, that was something the intelligence community handled, and the FBI; and maybe something Customs handled a little bit and border patrol, in protecting our borders; and the DOD handled—nothing we handled. And so, post- 9/11 we realized when we looked at what was happening in cells in New Jersey and New York, when we looked at what was happening in flight schools in Florida, we decided, if we train state and local cops to understand pre-terrorism indicators, if we train them to be more curious, and to question more what they see, and got them into a system where they could actually get that information to somebody where it matters…

"The responsibility for investigating terrorism still remains primarily with the FBI," he went on.

> They have the ability to interface with the intelligence community, to look at information that state and local cops can't look at, and probably shouldn't look at, don't need to look at. But we can get cops to understand how important their role is, how they are really the first line of defense, the eyes and ears on the ground when a bomb factory blows up and somebody thinks it was just a gas leak explosion. We were not looking for the right stuff, and so before it might get ignored and hopefully now it won't be ignored. Or they see people living in a sparsely furnished room with a lot of jihadist literature and other stuff that looks suspicious, maybe it is suspicious, or maybe it is just part of their religion. Or you know: people trying to take flight training to take off, but they don't worry about landing.

What was apparent, as I began this work, was that around this set of problems, a national intelligence apparatus was emerging. There was no relatively stable network though. Things and practices were in flux. Paul Rabinow, following Foucault, identifies the apparatus as "a specific response to a historical problem."[1] Foucault specifies a series of elements.

> [A] thoroughly heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions—in short, the said as much as the unsaid. Such are the elements of the apparatus. The apparatus itself is the system of relations that can be established between these elements.[2]

The idea had emerged that law enforcement has privileged access to the public, and this access, and the data that results, needed to be utilized. Cops were assumed to know their beat, to have acquired experiential knowledge of the residents, businesses, habits and characteristics of their neighborhoods. This familiarity is joined with a mandate to enforce

[1] Paul Rabinow, *Anthropos Today: Reflections on Modern Equipment* (Princeton: Princeton University Press, 2003), 54.
[2] Michel Foucault, "The Confession of the Flesh," in *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, ed. Colin Gordon (New York: Pantheon Books, 1980), 194.

the law, producing situations favorable to intelligence gathering in which law-breakers can be induced to become informants in exchange for lenience. Police officers' place in and knowledge of the social fabric indicated that they could go beyond being first responders at the scene of an accident or crime, to being also first preventers of terrorism. The cops I met were of a mixed mind about their proposed role in counterterrorism.[3] Some saw it as hype, others as a mandate. Some worried that the additional duties would impede their ability to do the basic work of policing. Others did not see it as different than what they already did. Or, they doubted that anything would actually change.

Practically speaking, I approached the apparatus by embedding myself in it, training as a criminal intelligence analyst, attending counterterrorism courses, and interning at Interpol. As an analyst in training, I was welcomed and met with conversation. Street cops and those at the fusion center saw themselves as the good guys, and were willing, often eager, to tell their stories. Joining in their work meant I was accepted generally as being on the same side. It could have been otherwise though. "It is a very tight-knit community, " one patrol officer told me,

> …(b)ecause you're dealing with certain aspects of humanity that the average person may see on the clip on the five o'clock news and forget about because it's dinnertime. When you go to a death of a child or something like that, you can't talk to people about it because they don't want hear it. That's why I hang with cops and firefighters, and nurses and ER doctors.

In addition to the internship as an analyst, one of my main forms of interaction with counterterrorism efforts was to attend Police Officer Standards and Training (POST) accredited courses on the topic. At the beginning of one class, the instructor asked if everyone was sworn law enforcement. I raised my hand. No, I was not. "Are you a hostage, a vacationer or an explorer?" he quizzed me, to laughter. Everyone who is in a training course, he told our group, fits in one of those categories. A hostage is someone who might not have any interest in the course content, but needed training credits. Or, a hostage could be an officer who didn't want to come, but whose boss said, "We need someone in the department to go." Because of this, there were train-the-trainer courses. These capacitated the attendees to return to their departments and teach a condensed version of the course, or at least be the go-to person on regulations concerning the topic. Vacationers are officers who needed credits as well, but had some time and/or funding, and thought the course location sounded like a good place to go. The instructor hoped, but was not hopeful, that most were in his last category. Explorers were "out to see what they could learn, whatever they don't know yet."

At trainings, attendees had coffee breaks and lunch together. In longer courses, especially those for which people had travelled to attend, the group would go out to dinner or drinks. They were state and local officers spread among a wide variety of law enforcement entities. When I asked if the seamless information network sought by the fusion center had yet penetrated the daily function of law enforcement, they responded, in the words of one, "for the way we really do business, nothing has changed." At the same time, most acknowledged that if they did happen to see a suspicious incident, there was now a person they knew to whom the information could be passed. The director was hopeful.

[3] As will be described in a later chapter, counterterrorism technically refers to proactive actions and antiterrorism, which has been subsumed under counterterrorism in popular usage, refers to preventative efforts.

> We learned that we had to get trained better as first responders. Especially the uniformed police community, they had to get trained better as first responders. We had to develop systems—which aren't fully developed yet but are still in process—to prevent stuff from falling through the cracks, to better really connect all the information. And we had to develop a system to report suspicious activity, and known terrorist activity, so that it gets to the right people: the FBI and other people that need to know it. That is why it is important to participate in fusion centers. That is why it is important to have terrorist officer liaison programs and training. That is why it is important for state and local law enforcement to participate with the FBI in joint terrorism task forces, why we need to invest in better information-sharing protocols.

His was a vision of law enforcement's role in counterterrorism. Interpol, when I interned at the General Secretariat, was also attempting to centrally position itself in the field by campaigning for terrorism to be dealt with as a crime. If terrorism could be policed, Interpol's importance, and funding, would increase. The organization was originally set up as a way for police to extend their reach beyond the borders of their own country by requesting assistance from another nation's police. In addition to facilitating communication, Interpol acts as a repository for information about crimes and criminals. Taking a political stand is against Interpol's charter; in as much as laws in most countries prohibit the same sorts of acts, however, Interpol defines crime as not being "political." Horizontal exchange through Interpol, bypassing diplomatic channels, rests on a presumption about the universality of crime, or at least the criminality of some acts. The implementation project worked towards universal implementation of laws that would criminalize a range of acts everywhere. "Biocriminalization" fit conceptually within the goal of strengthening Interpol's position, although institutionally the abstract project fit less well. There was conflict between the training and law-oriented thrusts of the project, as there was between the policing and legal aspects of the institution more generally. The director of the Bioterrorism project, who organized the regional trainings, never seemed clear on who I was or what I was doing, despite appropriate forms and protocols. The lawyer in charge of the latter, however, gave me a very necessary and helpful crash course in national and international legislation, and set me to work.

"Terrorism is a Crime"

> [The] assumption, shared by other hard-line lawyers in the White House counsel's office and in the Justice Department's Office of Legal Counsel, was that the criminal-justice system was insufficient to handle the threat from terrorism. There was consensus…that we had to move from retribution and punishment to preëmption and prevention. Only a warfare model allows that approach.[4]

In 2001, counterterrorism was generally understood in one of two ways. The Bush administration, together with select legal advisors in the Justice Department and the White House, counted it as one of the tools of war. In counterpoint, both abroad and domestically, some pushed for counterterrorism to be approached using tested law-enforcement practices that were strong in human intelligence collection, within the criminal justice system. On this view, which Interpol exemplified, terrorism was a crime and the

[4] Jane Mayer, "The Hidden Power: The Legal Mind Behind the White House's War on Terror.," *The New Yorker* 2006.

perpetrators criminals. As time went by, the criminal justice approach did not so much get stronger as it adapted, and hybrid forms developed.

The warfare approach, however, dominated in the years immediately after September 11, 2001. The attacks were defined as acts of war, and reprisal was authorized by Congress's Joint Resolution of September 14th. The Bush administration claimed the president's constitutional power to make war, and this power was expansively interpreted by the Justice Department. "The President," argued Deputy Assistant Attorney General John C. Yoo, now infamously, "has broad constitutional power to use military force" and "the President's powers include inherent executive powers that are unenumerated in the Constitution." In the last line of the last footnote of a memo, Yoo added,

> [W]e do not think that the difficulty or impossibility of establishing proof to a criminal law standard (or of making evidence public) bars the President from taking such military measures as, in his best judgment, he thinks necessary or appropriate to defend the United States from terrorist attacks. In the exercise of his plenary power to use military force, the President's decisions are for him alone and are unreviewable.

Yoo's memorandum, dated September 25, 2001, cited a 1824 Supreme Court decision.

> It may be fit and proper for the government, in the exercise of the high discretion confided to the executive, for great public purposes, to act on a sudden emergency, or to prevent an irreparable mischief, by summary measures, which are not found in the text of the laws.[5]

Yoo's argument was that if the President authorized something it was, in effect, legal no matter what. The unanimous court decision from which his citation is taken actually found that the government was liable for damages, even if motivated by perceived necessity.[6] Regardless of its legal sagacity, the Justice Department's interpretation of executive authority held for the duration of the administration.

The next significant executive position was that the situation called for preemptive measures. This was hotly debated as justification for a US invasion of Iraq, but with less fanfare also filtered into domestic measures. "Terrorism cannot be treated as a law enforcement issue," editorialized the *Wall Street Journal*, "in which we wait until the bad guys actually pull the trigger before we stop them."[7] The declaration, representative of a brand of counterterrorism rhetoric, conflated an argument and an assumption. That conflation provided a nexus, however, around which counterterrorism turned and developed. The argument was that terrorist acts must be prevented, rather than allowed to happen and then punished. The assumption was that law enforcement is only reactive. From its own origin stories of patrolling officers in London through fighting gangs, though, law enforcement has understood itself to be preventative.

[5] Lobel Jules, "The Commander in Chief and the Courts," *Presidential Studies Quarterly* 37, no. 1 (2007). John C. Yoo, "September 25, 2001 Memorandum Opinion for the Deputy Counsel to the President: The President's Constitutional Authority to Conduct Military Operations against Terrorists and Nations Supporting Them," ed. Department of Justice (Washington, D.C.: Office of Legal Counsel, 2001).

[6] *The Apollon, 22 U.S. (9 Wheat.) 362 362, 366-67*,(1824).

[7] "Editorial, the Limits of Hindsight," *Wall Street Journal*, 28 July 2003.

> In the FBI we have been told that prevention is now more important than prosecution. This is pure common sense and, as such, predated the recent terrorist events, especially with respect to violent crimes.[8]

The early idea was that police presence was a deterrent. A stronger version of prevention developed in relation to the mafia, other organized crime groups, and eventually drug traffickers. The tracking, documentation, use of informants and analysis, proponents argue, is actually the best preventative approach to counterterrorism.

In 2001, however, the criminal justice system, including the police, was considered inadequate to handle the threat, although not because of the traditional divide between domestic and foreign, or public and national security, which clearly was in a shambles. 9/11 made it evident that domestic attacks were possible, and by people legally and seemingly well established in the country. By extension, attacks could as well be from citizens as visitors. In addition, it was known that financial and logistic support activities occurred in the US and needed be addressed domestically. Yet, criminal intelligence was for a long time the poor cousin of national security intelligence, frequently ridiculed, in fact, as an oxymoron. Publications were limited to how-to manuals and training texts, and a few trade journals, equally oriented around practice. The result was a genre of activity at the core of law enforcement that was relatively unexamined and conceptually underdetermined. Police practices are shaped by the legal system within which they operate, which is to say that whether they follow them or not is explainable within this framework. Criminal intelligence is oriented toward producing concrete facts that can be assembled to support the assertion that someone has broken the law. This is largely, although not exclusively, the way that counterterrorism is done by police. They follow the clues of "supporting crimes" and add them to the counterterrorism apparatus.

"The primary differences," according to the Congressional Research Service, "between pure or traditional conceptions of intelligence and law enforcement intelligence lie in the following three areas: (1) the predicate for the intelligence activity itself, (2) intelligence clients and consumers, and (3) the legal regimes under which intelligence is collected.[9] These gradually began to merge, and in parallel the conceptualization of threat and law enforcement shifted, leading, in the course of four to five years, to a vision of integration between the systems. The first stage of this was the increasingly accepted idea that domestic intelligence was necessary in a time of a war. Domestic spying was legally curtailed, certainly for the CIA and in complex ways for the FBI. But instead of moving to a criminal justice model, the idea was that the criminal justice system and cops who wanted to keep their communities safe could nonetheless contribute information to the war efforts. By 2008, a RAND study partially inverted this formulation. The study looked at how terrorism ends and concluded that both intelligence and law enforcement were vastly more successful than war. They examined terrorist groups active between 1968 and 2006, and found that most (43 percent) ended by transitioning into the political process. For those that did not adopt nonviolent means (40 percent), RAND concluded, "policing is likely to be the most effective strategy." Both intelligence and police are better positioned to "penetrate and disrupt" terrorist organizations than the military, they argued.

[8] Coleen M. Rowley, "Oversight Hearing on Counterterrorism, Senate Committee on the Judiciary," (Washington, D.C.: FBI, 2002).

[9] Todd Masse, Siobhan O'Neil, and John Rollins, "Fusion Centers: Issues and Options for Congress," (Washington DC: Congressional Research Service, 2007), 91.

It is also easier to punish perpetrators for crimes such as drug trafficking, rather than terrorism preparations, which may be legal.[10]

Domestic Intelligence

If dealing with terrorism as an act of war has negative consequences, there are also problems with treating it as a crime, and engaging law enforcement as "first preventers." Domestic intelligence in the United States has a troubled history of abuse. In the 1970s, the Church and Pike Committee investigations traced the twin expansion of power and abuse over the previous decades. The US intelligence apparatus had been largely abandoned after World War I, and then reassembled circumspectly by Roosevelt in the buildup to World War II. During the war, Roosevelt placed responsibility for investigations of domestic espionage, sabotage and subversion with the FBI, and the Bureau held on to this prerogative. After the war, the CIA was officially assigned responsibility for foreign intelligence, with the explicit limitation that it "have no police, subpoena, or law enforcement powers or internal security functions."[11] With the FBI responsible for domestic intelligence and law enforcement, FBI Director J. Edgar Hoover greatly increased the size of his empire and there were but limited checks on the power of either agency.

During the Cold War and continuing through 1971, the FBI and CIA repeatedly violated their authority, often in arenas related to civil liberties. The CIA's Operation Chaos, for example, had the stated mission "to gather and evaluate all available information about foreign links to racial, antiwar, and other protest activity in the United States."[12] It also followed up on inquires from the FBI about Americans traveling abroad, and "amassed thousands of files on Americans, indexed hundreds of thousands of Americans into its computer records, and disseminated thousands of reports about Americans to the FBI and other governments."[13] The FBI's counterintelligence programs, the most famous of which is COINTELPRO, focused first on the Communist party, which had been stripped of "rights, privileges and immunities attendant upon legal bodies created under the jurisdiction of the laws of the United States" by the Communist Control Act of 1954. Techniques such as unlawful wiretaps and surveillance used against them were extended to groups that ranged across the political spectrum, from the Klu Klux Klan to the New Left. The "Rabble Rouser Index," for example, was a 1967 list of people who fomented racial discord, later expanded to those "with a propensity for fomenting" any disorder.[14] Ultimately the FBI targeted political figures that Hoover wanted to discredit.

Yet after 9/11, the question of *if* there should be a domestic intelligence apparatus was sidestepped by preponderant agreement that connecting and collecting the dots was essential. Specific programs that will be discussed later, such as the Pentagon's Total Information Awareness project, received publicity that seemingly served only as detours from any real debate, veering discussion from *if* to instead what form domestic intelligence

[10] Seth G. Jones and Martin C. Libicki, *How Terrorist Groups End: Lessons for Countering Al Qa'ida* (Santa Monica: RAND Corporation, 2008), 41.

[11] "National Security Act of 1947 (50 U.S.C. 403-3 (D)(1))."

[12] Brian A. Jackson, Darcy Noricks, and Benjamin W. Goldsmith, "Current Domestic Intelligence E," in *The Challenge of Domestic Intelligence in a Free Society : A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, ed. Brian A. Jackson (Arlington, VA: RAND, 2009), 34.

[13] Ibid.

[14] Ibid., 36.

should take. Put differently, the focus on information sharing avoided the question of what information and where it comes from.

From Collecting to Connecting the Dots

After fusion centers collect the dots, the next step is how they are connected, a combination of human and computer manipulation. Data-analysis and data-mining aim to turn information into intelligence. Some experts distinguish between subject-based, rule-based and pattern-based data mining.[15] Others propose a division into specific, relational or link, and general.[16] None of the labels perfectly categorize the different techniques, which can be and are combined into sequential processes.

"The problem," Jerome noted, "when you get to a large perspective is you get too much information."

> We have that flipside: information overload, which is a big thing. Maybe the biggest problem is information overload. There has to be way to scan the information properly and quickly and in a timely manner, and put it into actual, readable space. My thinking is if it takes you more than 3 sentences to explain something, your average cop isn't going to read it. Maybe your average person but I know your average cops won't because they don't think that far. You get to three sentences and if it doesn't have it all in there, it's gone. So we've got issues with that, that is going to be one of the things we fight once we have the information coming in. The discerning and sifting through the real information, what is usable to what is the chaff and needs to be set aside.

The ambition is to harness the mass of data instead of being thwarted by it, and to push forward to predictive power. The identification of patterns and development of models is also an attempt to overcome Roberta Wohlstetter's classic dilemma of signals and noise, warning and decision. The desire to preempt terrorism, to shift from reactive to pro-active, and from preparedness to preemption, impels research onto better, more powerful technologies.

A subject-based search or structured query begins with looking up a specific person, examining, for example, listed addresses and telephone numbers. This is what detectives and intelligence agents did manually, before the information was available for searching in digital form. Relational data-analysis looks for links between people or attributes, and is still a computer-aided version of standard criminal investigative practices, although more complex and proportionally more empowered by automation. "Of course, such a method must be used with care," one RAND study admitted.[17] "Given enough links, everyone would be on such a list." A search can also be conducted by attribute, instead of subject, or to seek relationships between attributes. For example, an analyst can create a list of rules to search databases for behaviors worrisome enough in

[15] "Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Assessment ", (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, 2008), 20-24.

[16] Martin C. Libicki and David R. Howell, "Privacy and Civil Liberties Protections in a New Domestic Intelligence Agency," in *The Challenge of Domestic Intelligence in a Free Society : A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, ed. Brian A. Jackson (Arlington, VA: RAND, 2009).

[17] Ibid., 177.

conjunction to warrant further investigation. Buying large quantities of explosives, firearms and stocks of provisions, given the violent history of the Branch Davidians in Waco, Texas, could warrant further investigation of individuals matching these criteria. Both subject and link analysis can be described as searches for patterns, including associations, sequences, classification, clustering.[18] They can be thought of as mining data for tactical or strategic intelligence. These are not, generally, new techniques but an enhancement of old ones.

The "data-mining" that is a major focus of concern, in contrast, "represents a difference in kind rather than degree."[19] It is "a discovery approach, in which algorithms can be used to examine several multidimensional data relationships simultaneously, identifying those that are unique or frequently represented."[20] A computer program can be created to automatically search for non-obvious relationships, a technique developed for Las Vegas casinos that has found security applications. At its extreme, predictive data-mining goes further. It takes up the social life of the population as functionally equivalent to the biological one, and expects that it will present natural patterns. This requires 1) massive quantities of data and 2) an assumption that such patterns exist. Previously, known patterns were needed for comparison, patterns extracted from history, from prior attacks, or at most invented possible scenarios. Patterns do exist for many kinds of crime, and for many other behaviors. The classic example is Amazon.com's comparison of one consumer's purchases to those of other buyers in order to suggest products. Similarly, credit card fraud is flagged by luxury purchases, rapid expenditures and buying things that can be easily fenced. The debate as far a technology goes is if there is such a pattern for "terrorism."

The director of the fusion center had a different kind of concern: "There's been a lot of technology development as a result of kind of the war on terror in the homeland security arena," he observed.

> But—and it's important—but the technology won't solve the problems, the real problems are political problems: how do we all agree to share information, how do we all agree to accept each other's clearances, how do we all agree what systems we will share in common?

Intelligence: Knowledge, Organizations, Activities

Intelligence encompasses surveillance and research, wrote Sherman Kent in 1949, those "attempts to establish meaningful patterns out of what was observed in the past and attempts to get meaning out of what appears to be going on now."[21] What is remarkable is both how consistent this understanding of intelligence has been, as well as the way in which it shows continuity from the very earliest uses of the word. Intelligence

[18] Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview," (Washington DC: Congressional Research Service, 2007).
[19] Ibid.
[20] ———, "Data Mining and Homeland Security: An Overview (Updated)," (Washington DC: Congressional Research Service, 2008), 1.
[21] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, N.J.,: Princeton University Press, 1966), 4.

comes from the Latin “to understand,” *intelligere*, and its roots are *inter* and *legere*.[22] Literally, it is to collect or choose between things. By 1390, in English usage this referred to an inherent ability to choose well, and to express this by word or speech. Intelligence was also understood to pertain to the branches of knowledge, forerunners of disciplines and scientific departments. By 1450, the word had added nuance. It could mean “knowledge of events,” especially of military value, as well as communication about those events. Thus early on, there was a producer of information, a recipient, and knowledge understood as a good, brokered between them. In the sixteenth century, the word came to refer to the communications of spies, secret or private agents. Secrecy had been introduced. Intelligence was not just the acquisition of knowledge but also a certain kind of practice, one that could involve deception to acquire it, or to keep it from others. By 1602, it was used for an agency that obtains secret information.

Kent, who will reappear in the next chapter, defined categories that corresponded closely to the various meanings the word had developed: knowledge, organization and activities. Intelligence for him was, first, a kind of knowledge. Second, it was the organization that produced that knowledge, meaning institutions and the arrangement between and within them. Third, intelligence was the result of activities or processes. Elaborating on the original meaning of collecting and choosing between things, collecting became today’s surveillance, “the many ways by which the contemporary world is put under close and systematic observation.”[23] Selecting, or sifting, as Frank put it, became research and analysis, the attempts to establish meaningful patterns.

Kent wrote pages on “intelligence is knowledge,” with descriptions of the types of intelligence a policy-maker might need, during war or peace. This should be organized by function, not in “an almost endless listing of the components of humanity and nature.”[24] What is unclear is if he followed his own advice, given his list of types: topography, environment, multiform permanent structures (cities, agricultural and industrial enterprises), people, status of the arts, sciences, technologies, and armed forces, character of the political system, economies, social groupings, codes of morality and “the dynamic interrelations which prevail among all of these.”[25]

His section on “intelligence is organization” contained a substantive and still pertinent analysis of US institutional relationships. “Intelligence organizations are in competition with each other,” he reminded readers. He took the contentious position that an intelligence agency should resemble a “university faculty.”[26] By this he meant that it should have access to references, be dedicated to scientific research and the goal of objectivity, and produce results that that indicate significance, and long-term trends. Such an agency must also “have many of the qualities of our greatest metropolitan newspapers,” which “watch, report, summarize and analyze” using well-placed sources, exercising editorial control, and meeting deadlines. Finally, it “must have certain characteristics of a good business organization,” by being “engaged in the manufacture of

[22] Inter means “among” or “between”, while legere can be “to choose” or “to gather, collect.” Intelligence is akin to the Greek *legein,* to collect, gather, choose, speak and *logos,* word, reason, speech, account. "Oxford English Dictionary," (Oxford University Press, 2005).

[23] ———, *Strategic Intelligence for American World Policy* (Princeton, N.J.,: Princeton University Press, 1966 (1949)), ix.

[24] Ibid., 4.

[25] Ibid., 6.

[26] Ibid., 75.

a product (knowledge) out of raw materials (all manner of data) and labor," and this product "must be packaged in a multitude of ways to suit the diversities of consumer demand."[27] Intelligence professionals, like all businessmen, must meet the needs of their consumers:

> They must study the market and develop its unexploited interstices. They must maintain small forces of decorous and highly intelligent salesmen who not only push the product and appraise the consumer reaction to it but also discover new consumer problems with an eye to the development of new products. They must plan for the future. [28]

Kent's compromise regarding the complex issue of how to organize intelligence analysts was that a "regional breakdown should be used as far as possible," with functional specialists (in economics, for example) at as specific a regional level as their knowledge permitted. He justified this strike against the traditional division of academic disciplines on the grounds that "if an economist who is thinking the French coal problem works with a political man who is thinking French politics the result is likely to be a better result than otherwise."[29] The need for regional specialists was widely agreed-upon, and affected not only CIA organization but also area studies and funding initiatives in academia still in place today.[30]

Kent's exposition of intelligence as an activity was not a lesson on how to overhear conversations or surreptitiously lift data, but rather an analytical method for producing what he hoped would be truly objective knowledge. Analysis was the core practice.

> After a confrontation of the problem and some decisions as to how it should be handled, there is a ransacking of files and minds for all information relating to the problem; and an evaluation, analysis, and digestion of this information. There are emergent hypotheses as to the possible aggregate meaning of the information; some emerged before, some after its absorption. No one can say whence came these essential yeasts of fruitful thought. Surely they grow best in a medium of knowledge, experience, and intuitive understanding. When they unfold, they are checked back against the facts, weighed in the light of the specific circumstances and the analysts' general knowledge and understanding of the world scene. Those that cannot stand up fall; those that do stand up are ordered in varying degrees of likelihood.[31]

Paraphrasing Kent's exposition, what comes first is the appearance of a substantive problem, which may be identified by someone who already knows a good

[27] Ibid., 76.

[28] Ibid.

[29] Ibid., 121.

[30] Disciplinary divisions seems to have crept back in, as Hedley reports that the CIA was re-organized into regional divisions by William Casey, Director of Central Intelligence under President Ronald Regan, p. 29. John H. Hedley, "The Evolution of Intelligence Analysis," in *Analyzing Intelligence: Origina, Obstacles, and Innovations*, ed. James B. Bruce and Roger Z. George (Washington, DC: Georgetown University Press, 2008).

[31] Sherman Kent and Donald Paul Steury, *Sherman Kent and the Board of National Estimates: Collected Essays* (Washington, D.C.: History Staff, Center for the Study of Intelligence Central Intelligence Agency, 1994).

deal, has an inquiring mind, and puts it to the task of potential problems. Alternatively, a problem may spring into relief as something new emerges. Or, it may come at the request of a consumer who, engaged in practical matters and negotiations, inevitably lacks some piece of information. The second stage is analysis of the problem, not only to discover and discard what is irrelevant, but also to shape the problem so that a solution will be applicable. Third is the collection of data, which may mean requesting it from someone who has it, or may initiate a surveillance operation to obtain the data. The fourth stage is evaluation of data. This, he notes, is complicated when the source of information is overly protected. He gives the pointed example of a French political figure's speech decrying the misery in a US-protected city in Algeria. In a report the speaker was rated "unreliable" because the evaluator knew the conditions were not that bad, but the real value of the report was that a supposed ally was promulgating "violent adverse criticism" and the issues of trust and trustworthiness this raised. Kent's fifth stage is the hypothesis. "[W]hat is desired," he expounds, "is…quantity and quality," so that there are as many interpretations of the data as possible. Kent contended, as everyone still does today, that too much security and internal rivalries block this from happening because these impede information from reaching the analyst. *How* alternative hypotheses are created, and what happens to them, is related to another important question: how intelligence supports policy and how policy directs intelligence. Kent noted that there was always the next-to-last stage, "more collecting and more testing of hypotheses" and gives his sixth stage as presentation of the hypothesis, "a new and better approximation to the truth."[32]

Kent excluded from his definitions of intelligence whole realms that others, even then, felt were integral. Intelligence meant strategic intelligence, the knowledge needed by policy makers as they devised and implemented national strategy. In Kent's optimistic assessment of future US actions, this was "the constructive knowledge with which we can work toward peace and freedom throughout the world, and the knowledge necessary to the defense of our country and its ideals."[33] Operational, tactical and combat intelligence were out, all of which have to do with immediate, situational knowledge for an operation or battle. He also excluded counterintelligence and "any other sort of intelligence designed to uncover domestically-produced traitors or imported foreign agents."[34] Anything in the United States or related to police function was ignored, although Kent was well aware of how fears of an "emergent American Gestapo" and bureaucratic territoriality negatively impacted the structure of the 1947 National Security Act. The act, he noted, specified that when the CIA "wants information which it feels may be possessed by the FBI, [the] CIA must ask for it in writing. In the best of circumstances this procedure constitutes a barrier between the two organizations, and in circumstances other than the best it can become an impenetrable wall."[35]

Some of the limitations that Kent imposed in his definition of intelligence came from the effort to differentiate his project from that of the Soviets. For them, "the concept of 'intelligence' embraces the broad range of Communist clandestine operations, which are made feasible by clandestinely procured information."[36] Kent argued long for a more scholarly approach, and deemphasized the covert operational activities of the CIA. In

[32] Kent, *Strategic Intelligence for American World Policy*, 151-79.

[33] Ibid., 3.

[34] Ibid.

[35] Ibid., 87.

[36] Ibid., xiii.

keeping with the wartime intelligence structure, he argued that clandestine activities should be understood as support provided by field officers to the home analysis group.

The issues Kent diagnosed with secrecy and policy still plague the intelligence community. Central Intelligence was conceptualized in its early days as a hub of information from the entire intelligence community on national-level concerns. Ideally, it produced on its own only what did not already exist. For this to really work, the CIA would have needed to be authorized to review everyone else's data. Final reports would not do. Such access would have to be enforced at the highest levels of government. This lacking, Kent correctly predicted that the CIA would embark upon its "own full-scale surveillance and research activities."[37] Competitiveness and isolation would lead to duplication of effort, and information would be hidden in the space between the CIA's "right to inspection" of intelligence from everywhere, and the special case of FBI intelligence, which would be "made available."

Kent was optimistic that the National Security Council, charged with reviewing operations, would exercise adequate control. The doctrine of plausible denial, which ultimately undermined this oversight structure, was far in the future. Covert actions eventually did not always pass through formal approval procedures, in order to shield high-level officials in case of public exposure. This protected politicians from the fallout of authorizing illegal or polemic actions, but also created a situation where agencies ran amok with little likelihood for accountability, and hence little incentive for self-regulation. So light a paper trail was left of CIA attempts to kill Fidel Castro that no one could ascertain if the CIA's actions had been authorized or not.[38] As a result, the House and Senate Select Committees on intelligence were established in the mid-1970s in order to better oversee covert operations. A document called a Presidential Finding was required for any proposed covert operation, which the intelligence committees could evaluate and discuss. Their internal review was designed to substitute for open public debate (incompatible with secrecy) on the desirability or advisability of a certain course of action.

Their evaluation would hinge, in part, on the congruence between available data and the planned course of action. Does intelligence indicate that the operation is necessary to some goal, likely to succeed, and better than an alternative? These are questions about the operation itself; they pertain to the means, as opposed to the ends. The other part of evaluation is the desirability of the goal, which might be to destabilize another country, or support an unsavory regime. The presidential finding is supposed to make a case for why a covert action should be taken, by the means proposed and for the desired end. Intelligence provides both the foundational support for this argument, and the occasion for fissure.

In a sense there is no "raw" data, as for any bit of information multiple evaluations pertain: on the reliability of the source, the possibility of error as well as deception, and potential effects. The fact that so much judgment is involved is at the core of the two most significant axes of dispute in intelligence: secrets and policy. The next chapter explores the development of national security intelligence through the life of Sherman Kent, and his part in the development of an intelligence apparatus during World War II. The involvement of US academics before, during and after World War II made the academic discourses of that time foundational to intelligence epistemology. The debates within intelligence paralleled, and for a period of time influenced, those that took place within the humanities

[37] Ibid., 101.

[38] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Dulles: Potomac Books, 2002), 130-31.

and social sciences. The intelligence establishment during the war actively debated the relationship between fieldwork and writing, practice and theory, and the puzzle of epistemological and moral relativism. Focusing on Kent's rendering of intelligence as it developed in the Research & Analysis Branch of the Office of Strategic Services during World War II, the next two chapters will focus on the debates over espionage proper, deception, counterintelligence and secrecy in general, and the appropriate relationship of intelligence to policy.

Chapter Two. Science and Secrets

Sherman Kent

The description of Sherman Kent as “larger-than-life” and his role as “the father” of strategic intelligence, when given by the Kent Center in the Sherman Kent School for Intelligence Analysis at the Central Intelligence Agency (CIA) University, combines to produce a tribute curiously public for a spy agency.[1] Although certainly “one of the architects of the US intelligence community,” as CIA literature describes him, the accolades position Kent as an avatar of the particularly American style of intelligence forged during the years of the Second World War.[2] In the Research & Analysis Branch of the Office of Strategic Services (OSS, forerunner to the CIA), two generations of scholars from across academic disciplines and throughout the political spectrum came together with the directive to apply a “positivist standard of objectivity” and produce tactical and strategic information to be used by the US government during and after the war.[3] The formative power of this intellectual and social experience influenced the work done in US intelligence and in academia for decades to come.

The ongoing homage to Kent, hand in hand with still-active detractors, stems from the canonical status of his 1949 book *Strategic Intelligence for American World Policy*. In it, he so ably expressed a version of intelligence that he and the book became synonymous with “the American view.”[4] Kent was a young professor and former graduate student in the Yale University Department of History when he was tapped to aid the US government in preparing for entrance into World War II. He brought with him the methods of scholarship in which he had been trained, resulting in his approach towards intelligence as a social science, a science of hypothesizing, testing and refining. For Kent and his World War II cohort, intelligence would be a work-in-progress that could produce the same incremental accumulation of knowledge as any other discipline, but that carried with it an additional standard of proof in its use in fighting the war. “Intelligence work is in essence nothing more than the search for the single best answer,” Kent stipulated, “upon which a successful course of action can be rested.”[5] The process, carried out by scientifically trained, rational minds, might be imperfect but was the best hope for estimating the future, and therefore to guide policy, available to any government.

Sherman Kent was not a radical innovator himself. He was a product of his times and the specific intellectual tutelage in the Research & Analysis branch of the OSS. He was what Paul Rabinow has called “a technician of general ideas.”[6] A capable and

[1] Dan Wagner, "Forward : Sherman Kent and the Profession of Intelligence Analysis," *The Sherman Kent Center for Intelligence Analysis Occasional Papers* 1, no. 5 (2002).

[2] Donald P. Steury, "Introduction," in *Sherman Kent and the Board of National Estimates : Collected Essays*, ed. Donald P. Steury (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1994), ix.

[3] Barry M. Katz, *Foreign Intelligence : Research and Analysis in the Office of Strategic Services 1942-1945* (Cambridge: Harvard University Press, 1989), 15.

[4] Kent, *Strategic Intelligence for American World Policy*; Shulsky and Schmitt, *Silent Warfare: Understanding the World of Intelligence*.

[5] Kent, *Strategic Intelligence for American World Policy*, vii-viii.

[6] Paul Rabinow, *French Modern. Norms and Forms of the Social Environment*, 2nd ed. (Chicago / London: University of Chicago Press, 1995).

assiduous scholar, he became dedicated to developing an epistemology of intelligence. A dedicated and sincere advocate for his craft, well aware of the changes his brand of intelligence represented, he provided a readable, synthetic articulation of the new intelligence. His book was designed for pedagogic use, aimed at the up and coming generation of intelligence practitioners. He was notably also a proponent of using academic standards, such as publishing and methodological, rigor for maintaining quality and incorporating improvements.

Kent's life bridged a period when universities and intelligence united for a time, developed in tandem, and then became disillusioned with each other. His antecedents aggregate many of the factors that affected how intelligence came to be defined in the United States: the practices of research and analysis, their institutionalization, and the focus on strategic results in the form of National Intelligence Estimates. With a privileged and sympathetic family, an elite education and connections, wartime experience, a quick pen, and writing support from the then-new War College, Kent became indelibly linked to intelligence's future. The path of his life, then, leads us through the development of the US intelligence apparatus, up to and continuing from the National Security Act of 1947.

***

> As has been said, historical research is much like research in the natural sciences. It consists of gathering facts—old and well known ones at first, and later, with the help of deeper knowledge of bibliography, new ones. It consists of forming hypotheses on the basis of these facts, of testing these hypotheses on the basis of these facts, of testing these hypotheses for traces of one's own ignorance or bias, of cleansing them if possible. The goal of research is to build better hypotheses than already exist and to establish them as relatively more true: it is to reveal a sharper picture of what happened and to make a closer approach to actuality than anyone has yet contrived. In the end, it results in giving to the world a new and original statement of what happened..."[7]

Sherman Kent, *Writing History* (1941)

Sherman Kent's father was a wealthy Yale-educated businessman who married the daughter of a professor. He took her to Chicago, where Kent was born in 1903, and then moved the whole family to California. Their sweeping property at the base of Mount Tamalpais would become the wealthy residential enclave of Kentfield, just north of San Francisco in Marin County. When the senior Kent ran successfully for US congress, the family maintained bicoastal residences. Sherman studied in Washington and at what would become the Thatcher School in Ojai Valley, California, which sent most of its students to Yale. His early school friendships, as well as the others he developed in his trajectory through the thoroughly aristocratic American educational system of the time, would reappear throughout his life in academia and intelligence.[8] This social web was in many ways the basis of the OSS, later the analytic branch of the CIA, and now the National Intelligence Center (NIC). Yale historian Robin Winks tellingly noted, "those who were suspicious of the OSS, perhaps thinking that it was a refuge for the socially well-to-

[7] Sherman Kent, *Writing History*, 2d ed. (New York: Appleton-Century-Crofts, 1967 (1941)), 34.

[8] Sherman Kent and Sally Newell Thacher, *Reminiscences of a Varied Life: An Autobiography* (Washington, D.C.: E.G. Kent, 1991).

do (since it contained more than its share of names from the social register), said that OSS stood for 'Oh, So Social,' 'Oh, So Swish,' or (since some also thought it was full of limousine liberals) 'Oh, So Socialist'."[9] Kent's privilege and wealth were standard for those in the Ivy League, and an Ivy League background was standard in the early era of US intelligence.[10]

"Sherm" was also known at Yale as "Buffalo Bill, the Cultured Cowboy," a reference to his California boyhood. Despite a lackluster undergraduate performance in which he notably did not pass introductory history on the first go-around, his combination of being personable, conscientious, and eager led professors to encourage him to pursue a PhD in history. As he began to focus on his studies, he received the distinction of being hired as a lecturer, before passing to candidacy, for the core freshman history class he had first failed. He went on to develop a course, first for undergraduates and then graduates, on "liberal and national movements of 19th century Europe." The father of US intelligence was actually considered a rather leftist specialist in the Enlightenment. His eventual dissertation topic and first book, published by Yale University Press in 1937, was on French "Electoral Procedure under Louis Philippe," and was described by a reviewer as concerned with exactly that: not the results of elections, but the injustice of the procedures by which men were denied suffrage.[11] Some critics of the Kent school of intelligence, self-identified students of Leo Strauss, would later disparage what they identified as its basis in the political tenets of the Enlightenment, especially the idea of the accessibility of truth to the common man, or anyone with access to scientific methods.[12]

Kent understood intelligence as almost coterminous with what he knew best, namely, history as a scientific endeavor. *Writing History*, his second book, was for students and detailed how to conduct independent research. History was thrilling to him, breaking new ground by practicing science to find out truths not about nature, but humanity. "Not that this pattern of progressive steps was new, nor even the general argument, for the method of history is closely akin to the method of science which Francis Bacon put forth in the early seventeenth century," he admitted. The new "use of the techniques of the natural sciences upon purely man-made evidence," however, was full of possibility, whether applied to the primary source documents of historical research or to vital papers snatched from an enemy nation, analyzed and transformed into intelligence.[13]

World War II became the applied arena for this vision of scholarship. Kent's words of guidance on historical research were slightly tweaked and reinscribed as methods of analysis in his 1949 *Strategic Intelligence for American World Policy*.[14] In his book on history he wrote, "we live in the middle of history. We consume as much history as air.... The doctor uses it in the diagnosis of symptoms; the businessman and the statesman use it when they reflect upon the smart move or the socially expedient move."[15] It was only a small switch to reapply this: "Intelligence is a simple and self-evident thing. In a small way

[9] Robin W. Winks, *Cloak & Gown : Scholars in the Secret War, 1939-1961*, 2nd ed. (New Haven: Yale University Press, 1996), 58.

[10] Ibid., 485.

[11] Edgar Packard Dean, "Reviewed Work(S): Electoral Procedure under Louis Philippe by Sherman Kent," *The American Historical Review*, October 1938.

[12] Gary J. Schmitt and Abram N. Shulsky, "Leo Strauss and the World of Intelligence (by Which We Do Not Mean Nous) " in *Leo Strauss, the Straussians, and the American Regime*, ed. Kenneth L. Deutsch and John A. Murley (New York: Rowman & Littlefield, 1999).

[13] Kent, *Writing History*, 6.

[14] Ibid; ———, *Strategic Intelligence for American World Policy*.

[15] Kent, *Writing History*, 2.

it is what we all do everyday. When a housewife decides to increase her inventory, when a doctor diagnoses an ailment...".[16] What changed were the ends, but not the means.

***

In 1941 President Roosevelt invited lawyer, businessman and World War I hero William J. (or "Wild Bill") Donovan to remedy the United States' lack of a centralized intelligence agency with global range.[17] "It seemed that Mr. Roosevelt," wrote Sherman Kent in his autobiography, "was far from pleased with the kind of intelligence support he was getting from the armed forces and was also inclined to disbelieve or give low credence to the political and economic information that was coming into the Department of State from its many diplomatic missions overseas."[18] Roosevelt wanted not just an intelligence organization, but specifically one attached to the Office of the President.[19] Donovan used his extensive contacts to staff what would become the Office of Strategic Services, described as bringing together "the functions of at least four British intelligence organizations," and in this twist of history with lasting repercussions, coming "far closer to combining all the purposes of intelligence than any democratic society had previously allowed itself in peacetime."[20]

Prior to the war, an intelligence agency such as the OSS was vigorously opposed in the United States. The country went through cyclical periods in which domestic surveillance was permitted, and each time curtailed because of abuses.[21] These episodes fueled on-going suspicion, which helped maintain strong support for states' rights and decentralized government. Information gathering and collation was therefore divided among the departments of State, Treasury, Navy and War, with agencies who specialized in specific topics or technical types of information. Pockets of foreign human intelligence expertise existed in parts of the Federal Bureau of Narcotics, Customs, and the State Department, but this could produce, at best, a piecemeal picture. The general population's opposition to top-heavy government and the rivalry between the extant intelligence groups were both factors that influenced how the US intelligence community was set up and developed.

The country's willingness to take up arms and eventually allow a centralized intelligence agency was in large part due to President Roosevelt's skillful capitalization of the Japanese attack on Pearl Harbor. Before that event, US participation in World War II was hotly debated. Roosevelt had campaigned on a promise of no foreign wars, and there was such strong domestic opposition that he was—and still is—accused of manufacturing the Japanese surprise assault, by purposefully goading them, ignoring intelligence, or both.[22] Many believed war was inevitable, but only after Pearl Harbor did the mood

[16] ———, *Strategic Intelligence for American World Policy*, vii.

[17] Barry M. Katz, "The Criticism of Arms: The Frankfort School Goes to War," *Journal of Modern History* 59, no. 3 (1987): 443.

[18] Kent and Thacher, *Reminiscences of a Varied Life: An Autobiography*, 186-87.

[19] Ibid.

[20] Winks, *Cloak & Gown : Scholars in the Secret War, 1939-1961*, 60.

[21] Morgan, *Domestic Intelligence: Monitoring Dissent in America* (Austin and London: University of Texas Press, 1980).

[22] Emily S. Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, ed. Gilbert M. Joseph and Emily S. Rosenberg, American Encounters / Global Interactions (Durham: Duke University Press, 2003).

change enough to make a declaration of war politically tenable. Thus the President quietly ordered the Office of Coordinator of Information (COI) into existence in July of 1941 (before Pearl Harbor), then transformed it into the OSS in June of 1942.[23]

When Kent described the initial situation in which COI was born, he wrote,

> From our visits and meetings with the various intelligence officers of the Armed Forces, we had some pretty solid evidence that any active intelligence work must have ended with the First World War. There were a lot of things that had changed in those twenty-three years, and, as far as anyone could determine, none of the operatives in the Army, Navy or the Marine Corps had done more than a lick or two to keep any of the files up to date. As much could be said for the State Department, with the sole exception of the Near East Division.[24]

His description is seconded in the official history of the OSS, written by Michael Warner of the CIA History Staff in the Center for the Study of Intelligence:

> Important and timely information went up the chain of command, perhaps even to the President, and might be shared across departmental lines, but no one short of the White House tried to collate and assess all the vital information acquired by the US government. State and the military developed their own security and counterintelligence procedures, and the Army and Navy created separate offices to decipher and read foreign communications. Senior diplomat Robert Murphy later reflected, "it must be confessed that our Intelligence organization in 1940 was primitive and inadequate. It was timid, parochial, and operating strictly in the tradition of the Spanish-American War."[25]

***

The OSS would become an all-purpose spy organization, with an on-the-ground presence around the world that included covert operations and counterintelligence. Yet the Research & Analysis Branch retained a distinctly intellectual bent. How did elite scholars become established at the heart of US intelligence? Part of the explanation is contained in Kent's description of the files he found when he started at COI: they were woefully outdated and the government needed primary information about the state of other countries in order to operate in them, or even simply to negotiate. Thus much of what the war apparatus needed was in libraries, the domain of scholars. Kent's pedagogical interest in teaching young minds how to do original research fit neatly into the task of collecting, sorting and compiling such data. Further, people with other skills or inclinations, or less choice, had been drafted into active duty, whereas scholars and their students still in school were available. Among these were European academics seeking refuge. They had expertise in regions of conflict, needed employment, and were invested in the outcome of the war. Finally, a number of established professors, well positioned in the small overlapping circles of wealth and privilege that existed between government,

[23] David A. Walker, "Oss and Operation Torch " *Journal of Contemporary History* 22 no. 4 Intelligence Services during the Second World War: Part 2 (1987).

[24] Kent and Thacher, *Reminiscences of a Varied Life: An Autobiography*, 197.

[25] Michael Warner, "The Office of Strategic Services: America's First Intelligence Agency," *Books and Monographs of United States Central Intelligence Agency*, no. May (2000), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/oss/index.htm.

Wall Street, and the universities, made the elements of an academic intelligence branch come together.[26]

In the many articles and books on the origins of the CIA and its “American” approach to intelligence, few note that as new analysts came out of the ivory tower of academia, the war was their first exposure to intelligence. This was, however, significant. “The London R&A outpost was a huge affair,” wrote Kent in his autobiography. “It was under the nominal control of Crane Brinton, a famous Harvard professor of history who had never had more than a moment's contact with the intelligence business before Langer packed him up and sent him off to run the London office. Here he was in charge of an office with thirty or forty members maintaining liaison with the British and other governments."[27] It was no wonder then that they crafted intell in the mold of what they knew, precisely because it was what they knew, rather than along the lines of the espionage-focused work done by other nations’ more established institutions. The “graduate student” approach would imprint the American conceptualization and institutionalization of the field. “Specialists” in a region had generally acquired their expertise in undergraduate language study, spent some time abroad, taken courses dealing with the region and then done narrowly focused graduate research on a specific topic. When the CIA moved into its permanent headquarters in Virginia, in fitting reference to both employees and aspirations it was called “the campus”.[28] In time Kent proposed, with eventual success, an intelligence institute after the manner of the Princeton Institute for Advanced Study, and a journal that would carry on a meta-conversation about the epistemology of intelligence, best practices and precise vocabulary.

Bureaucratically, the pre-Pearl Harbor Office of COI had been directly responsible to the president, although technically within the then-new Joint Chiefs of Staff system. Reorganization after Pearl Harbor put the transformed office in a position of needing to prove its worth to its unfavorably predisposed military overseers.[29] Operation Torch, launched in November 1942 against the Vichy French army of North Africa, was an early effort by OSS to muffle bureaucratic enemies and justify itself. The operation also provides a snapshot of what Research & Analysis did in the war. Efforts from the operational branch in Africa to Kent’s section in Research & Analysis exemplified the accomplishments and mistakes of the war office. They also illustrated many of the future strengths and weaknesses of US intelligence.

In his autobiography Kent recounts his group’s frenetic work of collecting and writing up a massive quantity of facts and suggestions to support the invasion. "Information on conditions Allied forces could expect to meet in North Africa, from the level of surf at the Casablanca beaches to details about North Africa's roads and railways, was all furnished on a lavish scale" and was widely praised for its accuracy and tactical usefulness.[30] However, notes historian David Walker, “American Military Intelligence, G-2, could have done the same job, as it had done similar jobs in the past,” and precisely in the arenas where the OSS claimed added-value, it seemed to fall short.[31] Almost all of their guerilla troops failed to meet their objectives, and, on the part of R&A, their prediction of

[26] Richard Harris Smith, *Oss: The Secret History of America's First Central Intelligence Agency* (Berkeley,: University of California Press, 1972).

[27] Kent and Thacher, *Reminiscences of a Varied Life: An Autobiography*, 212.

[28] Winks, *Cloak & Gown : Scholars in the Secret War, 1939-1961*, 60-115.

[29] Walker, "Oss and Operation Torch ".

[30] Ibid.

[31] Ibid.: 669.

the French response was wrong. Analysts had reasoned that because French resistance would amount to throwing in their lot with the Axis powers, they would instead capitulate easily, “allow American forces to occupy North Africa, and would perhaps even join the Allies.”[32] The French, however, fought back at full intensity. While "OSS personnel were correct in assessing that the French were fundamentally pro-Allied," notes Walker, "what they did not understand was that the French were also prepared to defend their own national interests, and would obey the orders of their leaders. OSS partially realized the importance of honour and obedience in the French army [but]...[t]he main problem facing French pro-Allied sentiment at the time of Torch was that there was no clear indication that the Allies would win the war."[33]

Although supporters claimed victory as proof of OSS usefulness, an alternative interpretation was that US success instead stemmed from two (unforeseen) serendipities. First, a French admiral who was visiting his polio-stricken son fell into American hands in Algiers. He had the power to order a French cease-fire, a necessary although perhaps not sufficient step to end the conflict. Second, and perhaps rendering the first superfluous, Hitler broke the 1940 armistice by invading the unoccupied zone of France (probably fearing that the French would go over to the Allies, and as a result provoking this reality). Yet by these coincidences, Operation Torch’s reputation was made. The genuinely effective contribution of the R&A branch had been the grunt effort to prepare information on the vital systems of strategic regions, culling libraries, government archives, newspapers and any other source of data written or human that they could find to create maps, tables and reports. In general, this was what one would now call “open-source” information, although data gleaned from an unsuspecting foreign visitor added to what was not available from library research. The utility of this information (some would say its preeminence over covertly acquired particulars) and the process of analytically weaving it together would become hallmarks of the CIA approach to intell for many years. This was part of the significant legacy of R&A, and Kent as the codifier of its efforts.

OSS influenced US intelligence in other ways as well. According to the scholar R. Harris Smith, briefly a CIA employee and subsequently a historian, “In a conscious effort to subordinate all political considerations to defeat of the enemy, OSS became very tolerant of the political left,” and those leftward leaning experts on Europe came with their own academic pedigree.[34] Barry Katz, historian of the R&A branch of OSS and its considerable intellectual legacy, describes how in the Washington, DC, headquarters of the OSS, “a cadre of the most outstanding Marxist scholars from the European emigration forged a tactical alliance with the executive wing of the US government.”[35] Leading theoreticians of the exiled Frankfort Institute for Social Research, including Franz Neumann, Herbert Marcuse, and Otto Kirchheimer, formed “one of the strangest of the illicit political liaisons of the 1940s.”[36] These intellectuals fleeing the Nazi regime, together

[32] Ibid.: 670.

[33] Ibid.: 674.

[34] This idea about the legacy of R&A is taken from Smith, but seems accepted by other authors. For example, an extensive 1974 review piece by Harry Howe Ransom discusses the scholarship, factual accuracy and opinions presented in Smith and four other contemporary works on the intelligence community, in which he summarizes Smith’s claims and does not raise issue with them. Harry Howe Ransom, "Review: Strategic Intelligence and Foreign Policy " *World Politics* 27, no. 1 (1974): 141-42; Smith, *Oss: The Secret History of America's First Central Intelligence Agency*, 9.

[35] Katz, "The Criticism of Arms: The Frankfort School Goes to War."

[36] Ibid.

with US academics from Sherman Kent's world, were joined and often managed by scions of US money society, the Mellons and Mellon in-laws, J.P. Morgan's sons, Vanderbilts, Duponts, and many others from Wall Street firms and oil companies.

Although OSS contained a remarkable spectrum of political beliefs, overt ideological bias in favor of a position or discrimination against that position was forcefully limited. "Donovan was as quick to defend his corporate officials, blue-blooded members of the establishment, and conservative émigrés," describes Smith, "as he was to protect his liberals, Socialists, and Communists."[37] This combination allowed a heterogeneous scene to develop within the OSS, at least some of which carried over to the (pre-McCarthy) CIA. This "ideological coexistence" was reputedly more successful in R&A than in the operational branches, where the endpoint was of course not scholarly objectivity but rather action that effectively achieved a goal. A certain percentage of wartime participants were captivated by the intellectual intensity combined with immediate real-world application, and, like Kent, either stayed with the agency despite its travails after the war, or returned within a few years. To counter the Soviet Union's support of Communist organizations around the world, these former Ivy League academics devised aid measures for moderates in other nations, "the non-Communist political left around the world— trade unions, political parties, and international organizations of students and journalists."[38] As odd as it may seem today in light of the conservative, homogenized reputation of the post-McCarthy intelligence community, critics of the CIA decried it as a liberal bastion, and indeed, this and FBI director Hoover's enmity was what eventually lead to drastic and damaging purges during the McCarthy years.

There were other formative carryovers from OSS days. In 1972, Smith wrote, "The Office of Strategic Services was the direct lineal ancestor of today's Central Intelligence Agency… The CIA is no aberrant mutation of 'Donovan's dreamers'; it is in many ways the mirror image of OSS."[39] One key aspect was that the "CIA inherited from OSS the crucial Donovan principle of merging Secret Intelligence and Special Operations in the same organization" and "the decision "was never seriously challenged when the CIA was created six years later."[40] Whether intelligence and covert operations should be housed together continues to be a matter of debate today. "Even more fundamental," according to Smith, "was the CIA's inherited justification for clandestine political operations unrelated to espionage and intelligence analysis."[41] The OSS foreign interventionism that was unquestioned in its moral justification against wartime fascism was neatly bequeathed to the CIA, and "The most notorious CIA-fomented coups in Latin America, Asia and the Middle East were, technically speaking, only extensions of Donovan's mandate for political warfare... [and] former OSS men who had once aided underground partisans became leading experts on counter-insurgency and the suppression of left-wing rebellions."[42]

***

[37] Smith, *Oss: The Secret History of America's First Central Intelligence Agency*, 15.

[38] Ibid., 368.

[39] Ibid., 361.

[40] Ibid., 361-62.

[41] Ibid., 362.

[42] Ibid.

The reports requisitioned from R&A during the war covered a vast range of topics, from trade routes to political structures, and "analysis" ranged from the production of tables of quantities and weights to subjective, if reasoned, plans for the future social structure of Germany. The Central European Section (led by Neumann, Marcuse and Kirchheimer), contributed "a minutely detailed picture of the social, economic, political, and cultural structure of totalitarianism, and its points of vulnerability and resistance within it."[43] Overall, the Branch's encyclopedic compilations of "facts" were better received than its reports providing "evaluation of 'objective possibilities' inherent in given situations."[44] Given its concentration of social theorists, jurists and scholars, the Central European Section's most direct effect was less on the war than on planning the peace, postwar governance and war crimes prosecution. Neumann, for example, argued against counting on psychological warfare (largely separated into a different branch of the OSS), because morale "is an inconsequential factor in the German situation and will continue to be so until military defeat smashes the elaborate system developed by Nazi-ism to control morale."[45]

For the future epistemology of intelligence though, it is equally important that R&A sustained a "theoretically explicit inquiry into the nature of objectivity" throughout its work.[46] Some direction came from Donovan, who recognized and supported the need to present an "impartial" product because of the politics of bureaucracy. The process of actualizing impartiality, however, necessitated an explicit epistemology and this was evident to the R&A coterie. They took up their own intelligence production as data for "basic analysis of the whole process of scientific thought in the social field," considered in reports with such titles as "The problem of objectivity in R&A Reporting" and "Memorandum Regarding Some Weaknesses in Our System of Research and Write Up with Suggestions How to Remedy."[47] The collected nationalities, socio-economic backgrounds, education and professions of R&A meant that there were diverse personal positions about the geopolitical turmoil of the time. From the war to Communist expansion and revolutions, many held differing opinions about what the future world should look like and how that should be achieved. Yet if their work were to have impact, and they were to survive bureaucratically, they needed to invent "a new mode of political writing."[48]

The Projects Committee was created in 1942 to put impartiality into practice. Some in R&A quickly decried its epistemological naïveté, arguing that "data do not exist outside of an interpretive framework."[49] Nonetheless, the committee monitored and edited output by pruning auxiliary verbs such as "ought" "should", and "must", exposing "subjective inflections posing as the views of unnamed foreign sources," withdrawing impolitic insinuations and removing rhetorical embellishments.[50] Subject to the demands of

[43] The Europe-Africa Division housed by 1943 these three, among others that included Hajo Holborn, Felix Gilbert, Richard Krautheimer, Henry Kellerman, Paul A. Baran, Eugene Fodor, Eero Saarinen and occasionally Friedrich Pollack and Arkadij Gurland Katz, *Foreign Intelligence : Research and Analysis in the Office of Strategic Services 1942-1945*, 34.

[44] Ibid., 18.

[45] Ibid., 38.

[46] Ibid., 15.

[47] Ibid. RG 226, Entry 37, Box 5: Projects Committee Correspondence; RG 226, Entry 1, Box 10; Moral File

[48] Ibid., 19.

[49] Ibid., 18-19.

[50] Ibid., 17.

customers, analysts were also forced to accelerate the pace of writing. If the historian Leopold von Ranke (whose historiographic methodology using varied primary sources was influential on the generation of historians in R&A) had "only wanted to show how it really had been," they needed to describe the present "as it was actually happening."[51]

The result was an experiment in the methodological issues of applied social science. These scholars, émigrés and American academics concentrated their considerable intellectual talents and training on the problem of knowledge in war. The lesson that "facts do not speak for themselves through a language of protocol-sentences that is transparent and politically neutral," was, according to Katz, "never fully mastered by the OSS, much less by the CIA," but was dispersed instead through those who left R&A to become the next generation of social science and humanities professors.[52] Perhaps logically, those who continued in intelligence maintained a practical concern with how to achieve objectivity and communicate it, rather than holding objections as to its impossibility. For them, writes Katz, "The antinomies of fact and value, scholarship and partisanship with which Max Weber had struggled so heroically had been largely resolved."[53]

More accurately, deep paradoxes of "objectivity" became matters of organizational structure and methodology. "This transformation of a group of obstacles and difficulties into problems to which the diverse solutions will attempt to produce a response" signals that intelligence was reproblematized.[54] On one level, what changed was the way "speech acts are taken to count in the register of true and false, as well as the ways in which such speech acts are produced and authorized," or the "mode of veridiction."[55] Intelligence became a profession and began an ongoing conversation about whether it was truly a science, a craft, or an art. The war analysts introduced new "ways of ordering interventionary practices," what Rabinow and Bennett have identified as the "mode of jurisdiction" and as intelligence practices were institutionalized, "a specified range of activities [was] discriminated as appropriate and subsequently ordered, i.e. organized in relation to one another."[56]

Academia continued to struggle with issues of objectivity, representation and responsibility, but within the CIA, a set of functional answers to these major epistemological questions were in place. Like the natural sciences, intelligence agreed upon a "mature doctrine," "difficult and important methodologies," and a "common technical vocabulary". Epistemology was considered settled and could be disconnected from methodology, which along with the bureaucracy of intelligence became the operative framework for problems. When insightful work was done by Richards Heuer, bringing to bear the advances of psychology on the cognitive process of analysis and biases, it was incorporated into the methodological paradigm.[57] Conceptual tools, such as the culture

[51] Jorn Rusen, "Rhetoric and Aesthetics of History: Leopold Von Ranke," *History and Theory* 29, no. 2 (1990); Katz, *Foreign Intelligence : Research and Analysis in the Office of Strategic Services 1942-1945*, 18-19.

[52] Katz, *Foreign Intelligence : Research and Analysis in the Office of Strategic Services 1942-1945*, 21.

[53] Ibid., 15.

[54] Foucault, "Polemics, Politics and Problematizations."

[55] Paul Rabinow and Gaymon Bennett, *A Diagnostic of Equipmental Platforms* (Berkeley: Anthropology of the Contemporary Research Collaboratory, 2007), 22.

[56] Ibid.

[57] Jr. Richards J. Heuer, *Psychology of Intelligence Analysis* (Center for the Study of Intelligence:

concept, continued to be used unchanged, despite anthropology's thorough dissection of this (formerly foundational) idea's epistemological limitations. American intelligence, largely—although not completely—cut off from outside input, continued its experiment in applied social science. It was in part because of this isolation that Heuer's work was received with such excitement within intelligence.

There were occasional critiques, and investigations (especially after notable failures), but the epistemology of intelligence was not again addressed as intensely or with such a rich background of knowledge as in the Research & Analysis Branch during World War II. Mostly, the practices and procedures developed during the war became routinized. The National Security Act of 1947 officialized institutional barriers. Concerns over or challenges to that system were often lost to immediate demands. The congressional or internal interventions that occurred nonetheless maintained the epistemology espoused by Kent, and accordingly changes were organizational and methodological.

The 9/11 Commission's conclusion that a "failure of imagination" was responsible for the events of September 11, 2001 is the sort of non sequitur that perhaps indicates emergent re-problematization. In the interim, however, an institutional correction was nonetheless supplied by the creation of the position of Director of National Intelligence and the Department of Homeland Security. Intelligence seems to have continued fundamentally unaltered and unchallenged, with one consequential and calamitous exception found in what may be called the "Straussian" school of intelligence.[58]

***

> If the Central Intelligence Agency insists on trying to perform the entire intelligence job and in so trying endeavors to reduce departmental organizations to impotence, it will not succeed. It will emerge from the battle perhaps still an agency but not central, and it may not even warrant the name intelligence. [59]
>
> Sherman Kent, 1949

The Research & Analysis Branch's supportive intelligence effort continued throughout the war and extended into preparation for the massive reordering and reconstruction of Europe. By 1944 the end of combat was foreseen; Donovan had already begun lobbying President Roosevelt to grant the OSS permanent status. The founding of an agency that could impinge on the powers of the military's Joint Intelligence Committee, Hoover's FBI, as well as the Department of State, was not, to be sure, unopposed. The technical means for different kinds of intelligence collection were still split between the Army, Navy, State Department and FBI (imagery, radio interception, cryptology capability, as well as regional expertise). The leaders of each were opposed to a general intelligence or "strategic information" service outside of their control, and united in their objections to a coordinator of information with any power over them. Their concerns included budget allocation, fears that confidential matters would be compromised, and also the control of information. Who would ultimately decide what intelligence the president would receive? Although none of the major intelligence players denied the need for centralized processing of intelligence, and all nominally agreed to the creation of the CIA, no one wanted to cede

CIA, 1999).

[58] Tom Barry, "The Neocon Philosophy of Intelligence," *Foreign Policy in Focus*(2004).

[59] Kent, *Strategic Intelligence for American World Policy*, 103.

turf or access. Knowing Donovan, they further feared the threat to their domains if he were left in charge.

FBI Director Hoover struck a blow in this bureaucratic battle by leaking a secret memorandum from General Donovan, written at the president's request, on turning the OSS into a permanent "central intelligence service." Presaging more recent (and now left-wing) opposition to intelligence, conservative journalists denounced it as a proposal for a "'super-spy system' in the 'postwar New Deal'," an "all powerful intelligence service to spy on the postwar world and to pry into the lives of citizens at home."[60] These sorts of power plays and public opinions did not stop intelligence's transition into permanence during peacetime, but the government had to take them into account.

When Truman took office after Roosevelt's sudden death, Donovan lost the leverage of a personal relationship with the president, which meant the OSS lost its advocate. "Well before those if us who had chosen to stay on had had the time to plan how the R&A Branch would fit into the post-war government and continue to contribute to the national cause," Kent recounted, "we read in *The New York Times* that General Donovan had been removed from the head position at OSS, and, in fact, the OSS itself had been disbanded. General Donovan himself also learned of these happenings from the newspaper."[61] Those employees who had not returned to their prewar employment, waiting in the hope of continuing in the heady intellectual environment of the OSS, were shuttled off to more conservative places in government, such as the regional sections of the State Department.

About a year later, President Truman proposed the Central Intelligence Agency. Two widely held understandings helped overcome the previous opposition to a centralized service. First, many of the multiple government reviews of Pearl Harbor accorded with the public assessment that it could have been avoided if there had been a central, coordinating group with both official and real access to all of the pre-incident intelligence. Second, as the war ended, the United States assumed a position as a major international power. Huge numbers of soldiers who were now familiar with abroad were returning. The newspapers carried daily reporting on the horrors of the war as revealed at Nuremberg Trials. Isolationists who had been against the entry into the war were in a weak position (but according to the official CIA historical account, still active) for arguing that the US should retreat behind its borders.[62] In early 1946 George Kennan's "Long Telegram" from Moscow warned, "World communism is like malignant parasite which feeds only on diseased tissue. This is the point at which domestic and foreign policies meet."[63] The argument that the country needed information to support worldwide action had become quite plausible.

Secrets

By the reissue of his book in 1966, Kent himself felt the need to address what he called the communist sense of the word "intelligence." He had been criticized for the all-source analytical approach; admitting that for the Soviets, his "overt intelligence" was "pretty much a contradiction in terms… [I]t is almost wholly espionage, counterespionage,

[60] Smith, *Oss: The Secret History of America's First Central Intelligence Agency*, 363.

[61] Kent and Thacher, *Reminiscences of a Varied Life: An Autobiography*, 223.

[62] Warner, "The Office of Strategic Services: America's First Intelligence Agency."

[63] George Kennan, "The Long Telegram," (Moscow: State Department, 1946).

and the fruits thereof."[64] One of his more vocal detractors was General Alexander Orlov, a high-ranking Soviet intelligence officer who defected in 1938, and lived in the United States until his death in 1973. Orlov published the *Handbook of Intelligence and Guerrilla Warfare* in 1963, which approvingly portrayed a Soviet emphasis on obtaining secret documents from other governments' files and disparaged Kent-style scientific analysis, especially as a gauge of nations' future actions.[65] He mocked such practices as being "but one step from mysticism and metaphysics."[66] A sympathetic review of Orlov's book in the internal CIA journal, declassified in 1993, eagerly championed this alternative to the social science version of intelligence:

> This Soviet preoccupation must be impressed on the American intelligence officer, who, in all likelihood, has been overtrained in the relative insignificance of covert information. American students of intelligence work—usually they are scholars and therefore committed to research—take pleasure in stressing that clandestine collection of information plays a rather minor role in the aggregate activity. The finished intelligence product, they say, usually contains not more than ten per cent of clandestine data.[67]

"In Orlov's opinion," wrote the anonymous CIA reviewer, who must have been somewhat frustrated with the dominant currents in US intelligence, "this Western reliance on overt information often leads to unprovable hypotheses and at the worst to wild leaps into the unknown."[68] Kent disagreed, protesting that "a single document or group of documents which contains the desired secret" can only be obtained, evaluated and used as the basis of a strategic decision together with "costly, voluminous, and subtle sorts of information and a lot of rigorous, thoughtful analysis."[69] While no one argued against the need to contextualize pieces of information, covertly obtained or not, Kent distinctly shifted analysis into position as the main activity.

[64] Kent, *Strategic Intelligence for American World Policy*, xiii.

[65] Aleksandr Ivanovich Orlov, *Handbook of Intelligence and Guerrilla Warfare* (Ann Arbor: University of Michigan Press, 1963).

[66] Winks, *Cloak & Gown : Scholars in the Secret War, 1939-1961*, 462.

[67] "Book Review of Handbook of Intelligence and Guerrilla Warfare by Alexander Orlov," *Studies in Intelligence* 8, no. 8 (1963).

[68] Ibid.

[69] Kent, *Strategic Intelligence for American World Policy*, xxiii-xxiv.

Chapter Three. Politicizing Intelligence

National Intelligence Estimates and the Iraq War

> [W]hereas knowledge of the objective situation is of highest desirability, any non-omniscient Being (i.e. Any frail human being) probably can never apprehend the true objective fact. He should, however, strive until it hurts.
>
> Sherman Kent, Strategic Intelligence[1]

> [O]bjectivity is not something to be valued in and of itself.
>
> Gary J. Schmitt[2]

In the CIA's first two years, the bureaucratic battle between extant intelligence groups and the new agency was fueled by a batch of CIA reports downplaying the danger of direct Soviet action and thereby undercutting support for military spending. Already antagonistic to their new competition in producing intelligence, the (also new) Department of Defense complained that CIA leadership was a "wild-eyed bunch of intellectuals whose colleges don't want them back."[3] Such disparagement, even if self-serving, gained credibility when the CIA failed to foresee Communist North Korea's 1950 invasion of South Korea. As part of the redesign of national intelligence, in late 1950 Sherman Kent accepted an invitation to return to government service, permanently resigning his professorship at Yale to join the Office of National Estimates. He ultimately became its director, and Chairman of the Board of National Estimates, a position he held until 1967. The Board, which by 1979 had morphed into the National Intelligence Council, produced National Intelligence Estimates, or NIEs. These reports were envisaged as data and thought-intensive research products that would synthesize for policy makers the "coordinated judgments of the Intelligence Community [IC] regarding the likely course of future events," providing the IC's "best analysis of specific issues of national importance."[4] The unchanged Kent-style orientation towards intelligence is notable even in these modern snippets, with their catchphrases of coordination, judgments on future events, analysis, and circumscription to issues of national importance.

Writing from the British perspective, Michael Herman notes that "intelligence as information is as old as government; so too is secret intelligence," but he identifies as hugely significant a shift that occurred in the mid-nineteenth century, when "the term also gradually came to be associated for the first time with government institutions established specifically for 'intelligence' purposes, separated from decision-taking and policy-making,

[1] Ibid., 41-42.

[2] Gary J. Schmitt, "Truth to Power? Rethinking Intelligence Analysis," in *The Future of American Intelligence*, ed. Peter Berkowitz (Stanford: Hoover Institution Press, 2005), 56.

[3] Smith, *Oss: The Secret History of America's First Central Intelligence Agency*, 366.

[4] "National Intelligence Council Mission," http://www.dni.gov/nic/NIC_about.html; Robert L. Suettinger, "Overview: History of Intelligence Analysis,"(2004), http://www.dni.gov/nic/NIC_tradecraft_overview.html. "National Intelligence Council Mission," http://www.dni.gov/nic/NIC_about.html

and distinct from the machinery of embassies and foreign offices which continued (and continue) to combine information-gathering with these executive functions."[5] Herman is not marking the development of intelligence agencies per se, which had long existed. He is emphasizing the independence of intelligence from policy, the development of a specific configuration "objectivity." "[U]ntil the mid-nineteenth century," he emphasizes, "there was little in the way of specialised, permanent intelligence institutions. Controlling collection and evaluating the results were integral parts of statecraft and military command. Intelligence as an institution was a Victorian innovation."[6] The British system is now often proposed as a model for the opposite reason, by American commentators who hold that its current formulation:

> encourages commingling in the belief that the best policy decisions are likely to result from a pooling of knowledge from among the country's international affairs experts. The British approach claims an additional advantage: policy officers brought into the analytic process are apt to view the finished intelligence products as more legitimate and acceptable since they have played an intimate role in their crafting.[7]

The US adopted the separation of intelligence and policy as the best practice, to be striven for if not always achieved, but the intersection of the two has been the site of significant dispute in the field. The ends of the spectrum are differentiated in their genuinely different beliefs about the character of knowledge.

Kent, representative of one end, accepted that even the most rigorous scientific methodology could not eliminate bias, but certainly the attempt was a virtue. Analysts needed to focus on producing the best information, not what would be done with it.

> [T]o wish simply for influence can, and upon occasion does, get intelligence to the place where it can have no influence whatever. By striving too hard in this direction, intelligence may come to seem just another policy voice, and an unwanted one at that.[8]

Kent did not mince words about situations where intelligence organizations were not administratively separate, that is, they were under the administrative control of its consumers in plans or operations. Every once in so often it will swing "into line behind the policy of the employing unit…, prostituting itself in the production of what the Nazis used to call *kämpfende Wissenschaft*, 'knowledge to further aims of state policy'."[9] In keeping with this concern, the Board, and indeed the Central Intelligence Agency, were designed to be structurally independent from policy makers. At a minimum, such handicaps to objectivity as direct administrative and financial control should be countered.

[5] Michael Herman, *Intelligence Power in Peace and War* (Cambridge, England ; New York: Cambridge University Press, 1996), 15.

[6] Ibid.

[7] Allan E. Goodman, Gregory F. Treverton, and Philip Zelikow, *In from the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence* (New York: Brookings Institution Press, 1996); in Shulsky and Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 139; Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven: Yale University Press, 1996), 129.

[8] Kent and Steury, *Sherman Kent and the Board of National Estimates: Collected Essays*, 42.

[9] Kent, *Strategic Intelligence for American World Policy*, 200.

The middle ground in the debate on the proper relationship between intelligence and policy is inhabited by intelligence professionals who accept the social science tack and ideal of objectivity, but have concluded that the timeliness and contextualization of an analytical product is compromised by too little policymaker contact. They suggest various models of integration with policy makers, such as embedded analysts who would "not be subject to the same tests of loyalty or ideological affinity that may be appropriate for 'political' appointees" or centers that blend intelligence and policy planning roles but retain "two distinct reporting lines."[10]

There is another school of intelligence at the far end in favor of integration with policy, which argues that analysis should "help the policymaker shape the future." This can be done by identifying opportunities to advance US interests, as well as the vulnerabilities of foreign elements, the factors subject to US influence; and the likely results of given US courses of action on foreign societies.[11] What may not be clear in this listing is the deeply divergent epistemology at its root. *Silent Warfare: Understanding the World of Intelligence* is a primer by Abram N. Shulsky and Gary J. Schmitt, widely praised and included on introductory intelligence reading lists. Shulsky, the original author, served the Washington establishment in different capacities over the course of his career, from the Senate Select Committee on Intelligence to researcher at the Rand Institute to the Office of the Under Secretary of Defense for Policy. He received his doctorate from the University of Chicago in 1972, and wrote the first edition of *Silent Warfare* (1991) based on a course he taught there in 1985, in order to present the "basic concepts and issues involved in the practice of intelligence."[12] Shulsky wanted to avoid narrow topicality, but following the book's publication he surmised that new laws and changes in the international political scene were of sufficient impact to indicate substantial revision, and he asked Gary J. Schmitt to take up the task. Schmitt had graduated from the University of Chicago in 1980, and also transitioned to government and policy. He succeeded Shulsky as minority staff director of the Senate Intelligence Committee, was executive director of the President's Foreign Intelligence Advisory Board under Ronald Reagan, and subsequently held a series of think-tank and contract positions, including teaching as an adjunct professor in International Studies at Johns Hopkins University. Perhaps most significantly, he was the executive director of the Project for the New American Century, an organization that advocated for US foreign policy of "global leadership" through military strength and moral clarity. The epitome of their message, communicated for years in letters, reports, op-eds and articles, were calls to depose Iraqi dictator Saddam Hussein.[13]

[10] James B. Steinberg, "The Policymaker's Perspective: Transparency and Partnership," in *Analyzing Intelligence: Origins, Obstacles, Ad Innovations*, ed. Roger Z. George and James B. Bruce (Washington, D.C.: Georgetown University Press, 2008), 88; James B. Bruce, "Making Analysis More Reliable: Why Epistemology Matters to Intelligence," in *Analyzing Intelligence: Origins, Obstacles and Innovations*, ed. Roger Z. George and James B. Bruce (Washington, D.C.: Georgetown University Press, 2008).

[11] Schmitt and Shulsky, "Leo Strauss and the World of Intelligence (by Which We Do Not Mean Nous) "; Kenneth L. Deutsch and John A. Murley, eds., *Leo Strauss, the Straussians, and the American Regime* (Lanham, MD: Rowman & Littlefield Pub.,1999); Jack Davis, "Improving Cia Analytic Performance: Analysts and the Policymaking Process," *Sherman Kent Center for Intelligence Analysis Occasional Papers* 1, no. 2 (2002), https://www.cia.gov/library/kent-center-occasional-papers/vol1no2.htm.

[12] Shulsky and Schmitt, *Silent Warfare: Understanding the World of Intelligence*.

[13] http://web.archive.org/web/20020607135927/www.newamericancentury.org/statementofprinciples.htm The group's Statement of Principles declares "The history of the 20th century should have

Shulsky and Schmitt also co-wrote “Leo Strauss and the World of Intelligence (by which we do not mean *Nous*),” a chapter in a 1999 tome on the political philosopher Leo Strauss’s legacy, and were the principal authors of a 1996 critique of intelligence performance, issued by the Working Group on Intelligence Reform of the National Strategy Information Center (NSIC), entitled “The Future of US Intelligence.”[14] These pieces (a third edition of *Silent Warfare* was published in 2002), plus Schmitt’s post-9/11 “Truth to Power? Rethinking Intelligence Analysis,” are expositions of their opposition to Kent on both theoretical and practical levels.[15]

Although Shulsky and Schmitt kept the basic categories of intelligence as “knowledge, organization and activity,” they took issue with placing analysis instead of espionage at the heart of intelligence, as well as the idea that intelligence should maximize objectivity by staying apart from policy makers. They argued that there is a peculiar and misplaced moral superiority associated with American post-war intell.[16] According to them, aspiring to place “international relations on a higher plane” ignores the reality of struggle between nations, and avoids the perhaps distasteful necessity of counterintelligence and deception. Analysis "as a variant of science and thus partaking of its prestige” gives too much credit to an imperfect methodology. They identify morality as one of the causes of a US preference for “clean” technical intelligence (technint) over “messy” espionage, but warn that technology, like science, gives an illusion of omniscience. They attribute the qualms of Americans about counterintelligence—such as domestic surveillance—to distaste for the reminder this entails that there is in fact an enemy, rather than to constitutional or “big-brother” government concerns. Shulsky and Schmitt disparage the inclusion of peripherals such as narcotrafficking for being remote from the core issue of struggle between nations. Worse, for them, is intell as a “morally neutral provider of information” rather than an information service for policy.[17] The purpose of intelligence for them is fundamentally the support of policy objectives, not the utopian goal of knowledge itself: “truth is not the goal, but only a means toward victory.”[18]

These points are all part of a cohesive counter school of thought on intell. It can be recognized in aspects of government that may otherwise seem peripheral, as in the resistance of the Pentagon to dealing with poppy cultivation in Afghanistan, despite

taught us that it is important to shape circumstances before crises emerge, and to meet threats before they become dire. The history of this century should have taught us to embrace the cause of American leadership”. They strongly advocated for war with Iraq after the attacks of September 11th, 2001. In their own words, which they put a September 20th, 2001 letter to then-President George W. Bush, “We agree with Secretary of State Powell’s recent statement that Saddam Hussein ‘is one of the leading terrorists on the face of the Earth….’ It may be that the Iraqi government provided assistance in some form to the recent attack on the United States. But even if evidence does not link Iraq directly to the attack, any strategy aiming at the eradication of terrorism and its sponsors must include a determined effort to remove Saddam Hussein from power in Iraq.”

[14] Schmitt and Shulsky, "Leo Strauss and the World of Intelligence (by Which We Do Not Mean Nous) "; Deutsch and Murley, eds., *Leo Strauss, the Straussians, and the American Regime*; Davis, "Improving Cia Analytic Performance: Analysts and the Policymaking Process."

[15] Schmitt, "Truth to Power? Rethinking Intelligence Analysis."

[16] Ibid., 167-68.

[17] They cite former DCIs Colby and Turner on the fascinating proposal of “free trade” intelligence, where benefits from vast quantities of information made available by technology are increased by its open flow and exchange.

[18] Shulsky and Schmitt, Silent Warfare: Understanding the World of Intelligence, 176.

arguments that opium provides critical funding for the violence that is more obviously in the military's domain. The contrast is Kent, for whom "Impartiality, not neutrality, is the key to the correct, proper, and just presentation of history within the bounds of systematic study."[19] In this he emphasizes that there should be equal consideration of possibilities, but the analyst should not ultimately withhold opinion on analytic decisions. Shulsky and Schmitt disagree on both accounts, that is, the goal of impartiality and that the place of analyst's work once it reaches the stage of opinion has any special value. Through the title of "Speaking truth to power?" Schmitt questions if this "speaking" is either feasible or desirable.

In this article Schmitt's pragmatic objections are readily accessible and historical. On the one hand, there is no unbiased truth, "Independence from policy making or budgetary preferences," he details, "does not guarantee objectivity. For much of the Cold War, for example, the CIA had an institutional interest in acting as 'the corrective' to Pentagon and military service estimates regarding Soviet military matters."[20] Not only was their accuracy no more guaranteed than the military, but their prestige and indeed relevance was "tied to this role" of dissident. A second problem Schmitt had with objectivity was that analysts develop positions in their areas of expertise, in which they are subsequently invested. Third, he argues that even attempts to build independence into bureaucracy are structurally flawed, because the CIA is not really independent, but ultimately subordinate to the president.

Given these limitations, analysts have no claim to truth, and therefore should not attempt to speak it to power.[21] Instead, they should collect the information policy makers need. Defensively, this includes different possible threat scenarios so that adequate preparedness policy can be devised: "a head's up about those things [the policy maker] should worry about and should possibly take action to head off." On the offensive, the analyst should seek out and work at "alerting policy makers of potential opportunities for taking advantageous action." The analysts' supportive effort requires that they be "sufficiently close to the policy process to understand policy objectives."[22] This is the reason "objectivity is not something to be valued in and of itself."[23]

Rather than try to conjure objectivity from analysts, Schmitt suggested letting "various analytic centers, working for different bosses, develop their own views on the same topic."[24] One of the correctives to intelligence frequently proposed is for these analyses to be coordinated, and "contribute to the preparation of a range of community products."[25] Or, the centers could produce alternative analyses for policy makers, whose responsibility and presumed competence is to make choices between them. "The downside usually tied to this suggestion," Schmitt admitted, "is that a policy maker will pick the analysis that fits his or her existing predilections. Yet given the speculative nature of many estimates in any case, there is no reason an experienced senior policy maker will

[19] P. 10 Kent, Strategic intelligence for American world policy.

[20] Schmitt, "Truth to Power? Rethinking Intelligence Analysis," 47.

[21] "Speaking truth to power" is a phrase that comes up repeatedly in writings by analysts on their profession.

[22] Schmitt, "Truth to Power? Rethinking Intelligence Analysis," 55.

[23] Ibid., 56.

[24] Ibid.

[25] Hedley, "The Evolution of Intelligence Analysis," 31.

not feel justified in trusting his or her own judgment, regardless of whether he or she is faced with one consensus-driven assessment or multiple competing ones."[26]

In Shulsky and Schmitt's version of the intelligence apparatus, the analyst must be part of the policy team, but cannot claim any special scientific authority in advising what the policy should be. Given their rejection of "objective" scientific methodology, it follows that unless the analyst holds the same or similar view on what "best" means, his or her work probably wouldn't be very useful. Or in other terms, if "truth is not the goal, but only a means toward victory," the prerequisite for victory as an objective is that the definition of victory is known. Their certainty is a clue. They are not simply proposing procedural improvements but rather are operating under a fundamentally different epistemology where there is a "right" way and it can be known (but not, they repeat, through social science). The unstated presuppositions underlying their practical concerns and solutions are grounded in a tradition of political philosophy that works with a different theory of knowledge than the one in which Kent-style intelligence is grounded. Intelligence, they agree, is produced via analysis, "the patient piecing together of bits of information to yield the outlines of the larger picture."[27] Often, analysis hinges "on such major questions as the nature and characteristic modes of action of a foreign regime."[28] In Shulsky and Schmitt's use of the word "regime", in their focus on morality in comparing "traditional" and "American" intelligence, and in their certainty of a specific truth, they signal their connection to the teachings of Leo Strauss.

> Studying political philosophy with Strauss proved to be a valuable counterweight to the doctrines that were then prevalent, not only in the academy, but in intelligence analysis as well. By emphasizing the distinction among regimes as the basic political fact, political philosophy prepared one for a much better understanding of the world than did the "scientific" social science, which sought to understand the various regimes in terms of universal categories.[29]

If a universal category assumes all people share a common human nature, Shulsky and Schmitt believe to the contrary that "the regime shapes human political action in so fundamental a way that the very souls appear different."[30] Ignoring the primacy of the regime leads to "explanations that rest on the subpolitical" and this is a fatal flaw if the political is the key to producing good strategic intelligence, and any knowledge of the social and political world more generally.[31]

It is perhaps not immediately clear why the category of regime and its Aristotelian types do not indicate simply another universal, or why the category of a country's regime would tell one anything about how its citizens actually live and think. Another Straussian, Eugene F. Miller explains as follows: Leo Strauss argued that sense data "given immediately or filtered through scientific constructs" cannot disclose the reality of social or political things. These things "come to presence in speech"; they exist because people talk about them, and therefore "social science must begin with speech," specifically, serious speech about matters vital to the community, the most fundamental of which is

[26] Schmitt, "Truth to Power? Rethinking Intelligence Analysis," 56. 56-57

[27] Schmitt and Shulsky, "Leo Strauss and the World of Intelligence (by Which We Do Not Mean Nous) ", 407.

[28] Ibid.

[29] Ibid., 410.

[30] Ibid., 409.

[31] Ibid.

"the question of who should rule." This brings us to the primacy of a regime, because (if this logic is accepted) it shapes "a community's way of life, its dominant patterns of thought, and its manners."[32]

A second key point is the rejection of value-free science. The decision about who should rule and the right form of government is understood to be a value judgment, of what are virtues and who is "best". If social science (and by extension, intelligence) forswears these kinds of judgments, "it is unable to make distinctions of morality or justice that are required to see regimes as they really are." One is forced to accept all governments as potentially equally valid. The paradigmatic example of this error (on this interpretation of Strauss's work) was the failure to recognize Hitler's government for tyranny.[33] If careful application of the scientific method leads to false objectivity, via a renunciation of value judgments, and yet Straussians champion "objective" truth, then there must be some other basis for non-relativistic epistemology. According to Strauss, it could be found through careful reading of the ancient Greeks, and "efforts to restore political philosophy as the quest for knowledge of political things as they are and as they ought to be."[34]

The classicist scholar M.F. Burnyeat reviewed a posthumous publication of Leo Strauss's essays in 1985, and an acrimonious exchange with the Straussians was begun, in which Burnyeat presciently observed: "The point, as I expressed it, was that 'something more than an academic quarrel is taking place' when Strauss defends his eccentric views. His misreadings of old books are not merely influential. They could have consequences in the real world of politics." Hadley Arkes, a Straussian professor at Amherst, endorsed such consequences, "The Straussians may supply a direction to Republican leaders, precisely because the teachings of Strauss are far more in accord with the sentiments of that broad public which has been bringing forth now a conservative majority."[35]

Noble Lies

Leo Strauss was doing research outside of Germany when the Nazis came into power. He made his way to the United States in 1938, where he taught political philosophy until his death in 1973. The largest block of this time (1949-1967) was in the Political Science department at the University of Chicago. This was the principal site from which he raised a generation of students who identified as conservative or neoconservative, many of whom went on to academia and government. Strauss is linked to esoteric writing, popularly described as his argument that "the works of ancient philosophers contain deliberately concealed esoteric meanings whose truths can be comprehended only by a very few, and would be misunderstood by the masses."[36] He contended that the risk of persecution compelled "all writers who hold heterodox views to

[32] Eugene F. Miller, "Leo Strauss: Philosophy and American Social Science," in *Leo Strauss, the Straussians, and the American Regime*, ed. Kenneth L. Deutsch and John A. Murley (New York: Rowman & Littlefield, 1999), 96.

[33] Ibid.

[34] ———, "Positivism, Historicism, and Political Inquiry," *The American Political Science Review* 66, no. 3 (1972): 817.

[35] Hadley Arkes, "Strauss on Our Minds," in *Leo Strauss, the Straussians, and the American Regime*, ed. Kenneth L. Deutsch and John A. Murley (New York: Rowman & Littlefield, 1999), 71.

[36] Seymour M. Hersh, "Selective Intelligence," *The New Yorker* 79, no. 11 (2003).

develop a peculiar technique of writing," one "in which the truth about all crucial things is presented exclusively between the lines."[37] An exoteric book contains "two teachings: a popular teaching of an edifying character, which is in the foreground; and a philosophic teaching concerning the most important subject, which is indicated between the lines."[38] The true esoteric message is disguised so that only careful readers might perceive it in the midst of a discourse that could well be diametrically opposite, or hidden in the speech of a disreputable character. It will be marked, however, by features that are enigmatic if one assumes a supremely masterful writer, who knew exactly what he was doing when he produced a text that contained "obscurity of plan, contradictions, pseudonyms, inexact repetitions of earlier statements, strange expressions."[39]

Of course, the question is, did Strauss himself write in this style? What his message was hinges critically on if one believes he did or not. Given the parameters he identified, there has been much debate on if he considered himself a heterodox writer, and if he considered himself at risk for persecution. Heterodoxy is integral to the Straussian mystique, so the answer generally given to the first part is *yes*: against the behavioralist orientation of Chicago political science he brought back the classical thinkers of political philosophy. On this level, the answer to the second question is also *yes*, as Straussians like to claim persecution from liberals for their endorsement of a common sense, self-evident morality. For Strauss himself, the answer depends on if his true message was anti-democratic. A passage, putatively interpreting Plato's Republic, might carry his real opinion: "the simply best regime would be the absolute rule of the wise; the practically best regime is the rule, under law, of gentlemen or the mixed regime," suggesting that a benevolent dictatorship by wise "philosopher kings" would be ideal, but second best would be for philosophers to guide kings from behind the scenes.[40] Most of his students argue that he thought that liberal democracy was the best option available but for this very reason he did not shy from critiquing it.[41] This defense does not actually deny that he thought a benevolent dictatorship would be better if possible, nor settle definitively if he thought that expressing this idea in the US would lead to persecution, and therefore employed esoteric writing.

Many of his students and their intellectual descendants have been in positions to influence or make policy, often on security, defense and intelligence. What Strauss meant, or more pragmatically, what his students took from his teachings regardless of what he sincerely believed, is therefore important. It is pointless to argue if Strauss's adherents correctly or incorrectly applied his teachings, or even what they were, especially in light of a doctrine of purposeful obfuscation. There are seemingly endless reports in the popular press, scholarly articles and books from all sides of that debate. What *is* of concern is how the understanding that was adopted from Strauss shaped a counter voice of intelligence.

The first point of agreement between supporters and detractors is that Strauss believed in the importance of absolute truth, good and evil.[42] This is not to say that

[37] Leo Strauss, *Persecution and the Art of Writing* (Glencoe, Illinois: Free Press, 1952), 24-25.
[38] Ibid., 36.
[39] Ibid.
[40] (NRH, 142-143 and Xenos, p. 133).
[41] Liberal, meaning favoring maximum individual liberty, and democratic, meaning leaders elected from the people, rather than from an aristocracy or by other criteria.
[42] Even among conservatives, many different and some contradictory lessons were drawn from Strauss. Gregory Bruce Smith summarizes accurately that "To date, various interpreters have asserted that Strauss's thought is a manifestation of everything from a naïve attempt to return to the Greek polis, to an elitist teaching regarding the existence of a rigid natural hierarchy that must

everyone agrees he believed in truth or good or evil, but certainly he held them to be useful. Eugene Miller, the Straussian political science professor cited before, argued that according to Strauss, value judgments can be "verified empirically," and are founded in "nature."[43] Miller does not quite state this directly, but instead uses a technique of inversion common to Straussians, stating that contrary to the traditional view (i.e. the ancient Greek view, via Strauss), positivism's reliance on science to verify assertions denies the possibility of knowledge of the good and just. The Straussian moral-epistemological position is, by inference: "there can be genuine knowledge of what is good and just, or of the standards ('ideals,' 'values') that ought to guide political choice."[44] This knowledge can be found in the Greek philosophical texts. Straussians believe that to find—to uncover—is actually a process of recovery, not interpretation. They aim to understand the ancient writings as their authors understood them. Unfortunately, contemporary seekers after knowledge cannot but reason through "the medium of concepts inherited from a complex tradition of political philosophy as well as the medium of the new natural science that emerged in early-modern times."[45] One must attempt to learn the style of thinking that preceded these misleading interventions in order to recover this "common sense" understanding that provides a basis for absolute truth.

Straussian epistemology is generally set up in contrast to positivism, and relativism (or in German tradition, historicism), which Strauss viewed as the dominant epistemological theory that had replaced positivism. Straussians consider Strauss's reading of Max Weber to be a definitive refutation of these other approaches to knowledge. From this base, they dispute the more accepted understanding of Weber as quite clear that science or any human pursuit of knowledge was not free from presuppositions. Weber wrote that "the capacity to distinguish between empirical knowledge and value-judgments" is necessary to the virtue of intellectual honesty, although he struggled with the inherent dilemma in attempting to make that distinction with tools that are themselves formed within the same ethical and epistemological system. [46] By the fact of that struggle, Weber can indeed be taken to represent another pole, opposite the idea that there is a fundamental truth to be found in nature or revelation, which indicates what "ought" to be.

For Weber, the most that science can do for someone is to "make him realize that all action and naturally, according to the circumstances, inaction imply in their consequences the espousal of certain values—and herewith—what is today so willingly overlooked—the rejection of certain others. The act of choice itself is his own responsibility."[47] This did not remove ethical considerations, to the contrary, Weber declared, "[t]he program to which we wish to adhere with ever increasing firmness" is "fulfillment of the scientific duty to see the factual truth as well as the practical duty to

be given direct political manifestation, to a conservative defense of modern, liberal capitalism, to a Nietzschean nihilism hiding behind an esoteric natural right teaching, to a Machiavellian atheism, to the efforts of a medieval rabbi in disguise" Gregory Bruce Smith, "Athens and Washington: Leo Strauss and the American Regime," in *Leo Strauss, the Straussians, and the American Regime*, ed. Kenneth L. Deutsch and John A. Murley (New York: Rowman & Littlefield, 1999), 103.

[43] Miller, "Leo Strauss: Philosophy and American Social Science," 816.

[44] Ibid., 817.

[45] Ibid., 816-17.

[46] Max Weber, "Objectivity in Social Science and Social Policy " in *The Methodology of the Social Sciences*, ed. E. A. Shils and H. A. Finch (New York: Free Press, 1904 (1949)), 58, 35.

[47] Ibid., 6.

stand up for our own ideals."[48] Yet science, or political philosophy for that matter, could not provide the content of those ideals. Who aside from big children, asked Weber, think that science could "teach us anything about the *meaning* of the world?"[49]

Strauss countered that Weber "never proved that the unassisted human mind is incapable of arriving at objective norms or that the conflict between different this-worldly ethical doctrine is insoluble by human reason."[50] He contended that the scientific attempt to grasp things as they really are is defeated by the subjective evaluation inherent to observation. Any attempt to remove that element of judgment in pursuit of objectivity reduces reasoning to reflexivity, human processes to historical artifacts. Strauss, explaining political philosophy (which was, for him, first among the social sciences and a surrogate for knowledge generally), said,

> All political action is concerned with either preservation or change. When it is concerned with change it is concerned with change for the better. When it is concerned with preservation, it is concerned with avoiding something worse. Therefore all political action presupposed opinions of better and worse. But you cannot have an opinion of better and worse without having an opinion of good or bad.[51]

If one's judgments are historically conditioned, relative to time and place, then "modern science is merely 'one historically relative way of understanding things which is not in principle superior to alternative ways of understanding."[52] Within this relativistic epistemology, there can be no absolute basis for truth, which, for the Straussians, is theoretically untenable.

"When you see that you follow an opinion, you are by this fact driven to try to find knowledge, to replace opinion by knowledge."[53] The true lovers of knowledge are the philosophers, and this leads to Strauss's discussion of classic natural right, which is the basis for the accusations of masked anti-democratic lessons in his writing. Following Plato, men are divided into wise (philosophers), gentlemen (rulers) and the vulgar. Decisions should be the province of philosophers, in order to rule, or, second best, provide guidance to the policy-making rulers of the unwitting common man. The accusations against the Straussians (Paul Wolfowitz and Abram Shulsky are commonly named, among others) is that they position themselves in this "natural inequality" as the philosophers, best suited to advise the rulers and arbiters of real right and wrong.

Philosophers, as advisors, are justified in using "noble lies," as well as hiding "the still more noble truth" in their esoteric writing.[54] Strauss of course did not announce that he wrote in this way, but offered that for fellow philosophic readers, the esoteric writer "would do almost more that enough by drawing their attention to the fact that he did not object to

[48] Ibid., 58.

[49] ———, "Science as a Vocation," in *From Max Weber: Essays in Sociology*, ed. H. H. Gerth and C. Wright Mills (New York: Oxford University Press, 1946), 16.

[50] Leo Strauss, *Natural Right and History*, Charles R. Walgreen Foundation Lectures (Chicago: University of Chicago Press, 1953), 70.

[51] Leo Strauss, lecture at the University of Chicago in Spring 1966, quoted in George Anastaplo, Leo Strauss at the University of Chicago p. 9

[52] Miller, "Leo Strauss: Philosophy and American Social Science," 93.

[53] Leo Strauss, lecture at the University of Chicago in Spring 1966, quoted in George Anastaplo, Leo Strauss at the University of Chicago p. 9

[54] Strauss, *Persecution and the Art of Writing*, 35-36.

telling lies which were noble, or tales which were merely similar to truth."[55] Certain opinions and truths "must remain the preserve of a small minority."[56] Philosophers must conceal these "from all but other philosophers"; both rulers and the masses are subject to this deception, for their own good. Noble lies are permissible, even "one's social responsibilities" when used to hide a too-harsh truth, or accomplish that which is necessary or good, but that not everyone will understand.[57] For Shadia Drury, a prominent academic opponent of the Straussians, this is both an impoverished understanding of Plato's concept of the noble lie and one of the keys to Strauss's esoteric message. His doctrine, in her words, is that:

> the masses need myths and illusions. They need to believe that is an unchanging moral law sanctioned by a divine creator and backed by the powers that be. If the vulgar were to discover, as the philosophers have always known, that God is dead, they might behave as if all is permitted. Strauss does not say all this explicitly because a wise person ought not to say publicly that there is no God and no unchanging moral law. Genuine philosophers know that people's love of knowledge has brought them only grief. But modernity succeeds in making things worse by bringing philosophy to the masses. Nothing, says Strauss, separates the ancients from the moderns more than the attitude they have "noble (or just) lies" and "pious frauds."[58]

Schmitt and Shulsky cite Strauss's theory of esoteric writing as a reminder that deception is widespread and must be taken into account. His claim that the "common sense understanding of political things is primary" points them towards the regime as a lens for intelligence.[59] If "human things cannot be understood apart from judgments of good and bad," then the fact-value distinction is a false premise for intelligence analysis.[60] A morally neutral scholarship, including intelligence, cannot perceive a regime for what it is, and will be blind to what its actions indicate.

Iraq

The United States' 2003 invasion of Iraq was predicated on intelligence reports that the country had prohibited weapons with mass destruction capabilities (WMD).[61] In the early months of the war, soldiers and inspectors scoured the country for weapons they were sure they would find, but were not successful. It became clear that the collective assessment of the world's intelligence agencies had been wrong. On the part of the US, the 2002 NIE *Iraq's Continuing Program for Weapons of Mass Destruction,* "one of the most high-visibility and policy relevant NIEs in years" had deeply erred, missing four out of five key assertions.[62] In the face of such a monumental mistake, many suspected that the

[55] Ibid.
[56] Leo Strauss, *On Tyranny*, 26.
[57] Strauss, *Persecution and the Art of Writing*, 35-36.
[58] S. B. Drury, "The Esoteric Philosophy of Leo Strauss," *Political Theory* 13, no. 3 (1985): 331-32.
[59] (Schmitt, in Miller).
[60] Miller, "Leo Strauss: Philosophy and American Social Science," 816.
[61] "National Intelligence Estimate on Iraq's Continuing Program for Weapons of Mass Destruction," (2002).
[62] Bruce, "Making Analysis More Reliable: Why Epistemology Matters to Intelligence," 182. James

White House had manipulated evidence to get authorization for a war that they wanted. Suspicions began to circulate in the popular press that "a small cluster of policy advisers and analysts… based in the Pentagon's Office of Special Plans [OSP] had co-opted the intelligence process.[63] They were accused of dismantling "the existing filtering process that for fifty years had been preventing the policymakers from getting bad information, creating "stovepipes to get the information they wanted directly to the top leadership."[64] The group, in the Office of the Under Secretary of Defense for Policy, was reported to have instigated the war with skewed assessments fed to the Administration and leaked selectively to the press. The "alternative analyses," as they were later defended, set great store by later discredited informants, in suspect data about Iraq's weapons development and presented overly favorable outcome scenarios for a post-war Iraq.

If the prohibited weapons had been found, the Straussians might have remained active but unobtrusive participants in government and political circles. In 2003, however, Paul Wolfowitz was the Deputy Secretary of Defense. He had authorized the creation of the Office of Special Plans, of which Shulsky was the director until he shifted from within the Office of the Under Secretary of Defense for Policy to the Office of Northern Gulf Affairs.[65] Schmitt, on his part, had been publicly advocating preemptive action against Iraq for years via the Project for the New American Century (Wolfowitz and Shulsky, as well, were members). There were many other actors in the build-up to the war, and also other intellectual influences even on the Straussians, such as the Chicago-based defense strategist Albert Wohlstettor. The events and Strauss's reputation, however, put Shulsky and Schmitt's statements in a different light. Leo Strauss, they had written, alerted them to

> the possibility that political life may be closely linked to deception. Indeed, it suggests that deception is the norm in political life, and the hope, to say nothing of the expectation, of establishing a politics that can dispense with it is the exception.[66]

The imputation in the media, and later by irate members of congress, was that some people in the Administration wanted war with Iraq, and not only cherry-picked analyses that supported it, but in order to do so had set up competing centers in the Pentagon so that trusted people could produce those analyses.

A congressional investigation was launched in the summer of 2003 to ascertain why the intelligence community had been wrong, or if it had been politically pressured into its false results. Phase I found fault was found throughout the intelligence community, although as primary drafter of the National Intelligence Estimate, the CIA bore responsibility. The investigation reported that "analysts began to look for evidence that Iraq was expanding WMD programs. Analysts interpreted ambiguous data as indicative of the active and expanded WMD effort they expected to see."[67] Everyone already thought

B. Bruce, "The Missing Link: The Analyst-Collector Relationship," in *Analyzing Intelligence: Origins, Obstacles and Innovations*, ed. Roger Z. George and James B. Bruce (Washington, D.C.: Georgetown University Press, 2008). 201

[63] Hersh, Selective Intelligence

[64] Kenneth Pollack, in Hersh, the stovepipe

[65] Barry, "The Neocon Philosophy of Intelligence."

[66] Schmitt and Shulsky, "Leo Strauss and the World of Intelligence (by Which We Do Not Mean Nous) ", 410.

[67] "Report of the Senate Select Committee on Intelligence on the U.S. Intelligence Community's Prewar Intelligence Assessements on Iraq Together with Additional Views," (Washington,

they knew the answer: “The presumption that Iraq had active WMD programs was so strong that formalized IC mechanisms established to challenge assumptions and ‘group think,’ such as ‘red teams,’ ‘devil’s advocacy,’ and other types of alternative or competitive analysis, were not utilized.”[68] Under a 21-day deadline, they had quickly updated a previous NIE, but little new data had come in, and most of that turned out to be wrong. The analysts and their managers were accused of sharing policy-makers’ mindset, thereby distorting their analyses, but in the absence of new data there was little to provoke a significant shift. The Butler Report on British intelligence, which along with other European nations had equally failed, doubted that any other judgment could have been reached. It would be difficult to imagine, they said, “in terms of good analytical tradecraft as opposed to a blind leap of faith, how an assessment might have been written that would have come to the conclusion that Saddam was telling the truth and that Iraq did not have WMD in 2002.”[69]

Thus the Phase I report accepted that the faulty 2002 NIE covered the major reasons given for war, and found no evidence of overt political pressure. The Intelligence Community’s own errors of data evaluation and analysis were to blame. Yet the intelligence cited at the time that arguments were being made to go to war had been classified, and therefore the public and much of congress had not been in a position to evaluate it. Phase IIa, however, laid out exactly which statements justifying the invasion had not been substantiated by mainstream intelligence. The discrepancy completed the circle back to the origin of the information, and although the Under Secretary of Defense roundly denied it, multiple fingers pointed back at the Pentagon, the policy office and its subunits.

As Gregory Treverton, a RAND scholar who was vice chair of the National Intelligence Council (which produces NIEs) in the first Clinton administration, noted dryly, “There is no evidence that the Pentagon operation had a direct effect on the October 2002 NIE, but its perspective became part of the broader intelligence in the run-up to war, supporting political arguments that the mainline intelligence agencies did not.”[70] Phase IIa pointed to the gap between what had been supported, even incorrectly, by intell and what senior Administration officials had claimed. There was (mis)information and no source. The Select Intelligence Committee requested a Department of Defense’s internal investigation. The “Review of Pre-Iraqi war activities of the Office of the Under Secretary of Defense for Policy" concluded that the Office of the Under Secretary of Defense for Policy had:

> developed, produced, and then disseminated alternative intelligence assessments on the Iraq and al-Qaida relationship, which included some conclusions that were inconsistent with the consensus of the Intelligence Community, to senior decision-makers. While such actions were not illegal or unauthorized, the actions were, in our opinion, inappropriate given that the products did not clearly show the variance with the consensus of the Intelligence Community and were in some cases, shown

DC2004), 18-19.

[68] Ibid., 21.

[69] Mark M. Lowenthal, "Intelligence in Transition: Analysis after September 11 and Iraq," in *Analyzing Intelligence: Origins, Obstacles and Innovations*, ed. Roger Z. George and James B. Bruce (Washington, D.C.: Georgetown University Press, 2008).

[70] Gregory F. Treverton, "Intelligence Analysis: Between "Politicization" And Irrelevance," in *Analyzing Intelligence: Origins, Obstacles and Innovations*, ed. Roger Z. George and James B. Bruce (Washington, D.C.: Georgetown University Press, 2008), 95.

> as intelligence products. This condition occurred because the OUSD(P) expanded its role and mission from formulating Defense Policy to analyzing and disseminating alternative analysis.

The Under Secretary's office defended itself by arguing that their policy office produced informational briefs to assist in developing policy, not intelligence. Their explanation rested on the definition of intelligence. Only a full process of validation, correlation, analysis, interpretation, presentation and dissemination, can be considered intelligence, and so they claimed it a distortion to label a single activity, such as analysis or interpretation, as "Intelligence Production."[71] Phase IIb tried to trace the trail back, but was unable to prove wrong-doing.

Gannon describes the distortion of analysis as having "two well-established forms—politicization and analytical bias. Politicization, the willful distortion of analysis to satisfy the demands of intelligence bosses or policymakers" and bias, "a subtle but pervasive influence based on the unconscious exertion of pressure."[72] Treverton adds that politicization can include "commitments to perspectives or conclusions, in the process of intelligence analysis or interaction with policy, that suppresses other evidence or views or blinds people to them."[73] Some speculated that those working in the Pentagon's policy offices had been captives of their convictions, developing analyses from a position of ideological certainty that matched that of the bellicose administration. Others interpreted Strauss's writings on the role of philosophers as advisors to rulers, and the legitimacy of the noble lie for the greater good to suggest that the analysts engaged in bad faith collusion, manipulating data to buttress a policy they already supported, and giving it to those in power.

If a primary, common sense understanding of political things is used, "the mind can grasp nature as it is and, on the basis of such knowledge, apprehend what ought to be."[74] Behind Schmitt's argument that "Our Basic Instincts Were Sound" in a *Los Angeles Times* opinion piece defending the US invasion of Iraq was this "common sense" understanding, and the primacy of the regime. "What we lack in detailed intelligence about weapons programs is more than offset by our strategic intelligence about particular countries' intent."[75] Kent spoke directly to this possibility, stating with some acerbity,

The procedure which moves from the known to the unknown with a certain amount of tentative foraying as new hypotheses are advanced, tested, and rejected is merely the most respectable way. Its very opposite is sometimes employed, though usually with a certain amount of clandestinity. The follower of this reverse method first decides what answer he desires to get. Once he has made this decision, he knows the exact locus of the apex of his pyramid but nothing else.[76]

[71] Directive No. 5105.21 paragraph E2.2.3

[72] John C. Gannon, "Managing Analysis in the Information Age," in *Analyzing Intelligence: Origins, Obstacles and Innovations*, ed. Roger Z. George and James B. Bruce (Washington, D.C.: Georgetown University Press, 2008), 221-22.

[73] Treverton, "Intelligence Analysis: Between "Politicization" And Irrelevance," 93.

[74] Miller, "Leo Strauss: Philosophy and American Social Science," 817.

[75] Gary Schmitt, "Our Basic Instincts Were Sound," *Los Angeles Times*, 1 February 2004.

[76] Kent and Steury, *Sherman Kent and the Board of National Estimates: Collected Essays*. theory of intelligence

PART II

POLICING TERRORISM

Chapter Four. Tracking the Biological Weapons Threat

Weapons of mass destruction have the *World at Risk*, declared the arrestingly titled report from the US Commission on the Prevention of WMD Proliferation and Terrorism, published December 2008. They opened with the claim that it is “more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013.”[1] Biological weapons, they added, were the most likely terrorist choice. Exactly what “biological weapons” refer to, what they threaten and how they have been imagined and contained within the realm of international law (and correspondingly, the avoidance or enforcement of those laws) will be addressed in this chapter.

There are much-repeated examples of how biological weapons have existed since time immemorial: plague-ridden corpses were thrown over city walls during the 1346 siege of Caffa (now Feodosia, Ukraine); Pizarro passed smallpox-contaminated clothing to South Americans in the 16th century; British commander Sir Jeffrey Amherst infected blankets during the French-Indian War (1754–1767). These can be counted as weapons only a loose sense though, one frowned upon by most military historians, in that they were tools of total war used to target the civilians. They lack the industrial age mechanization of disease, or the later equation of biological weapons with existential threat.

As well, what has been understood as the target or object of bioweapons has been unstable. In the pertinent international accords, the object shifts variously between international order (biological weapons would unbalance relations between nations), soldiers on the battlefield, the civilian population of a country at war, and the civilian population at risk of terrorist attack. At this point, many have come to assume that the real problem with these weapons is their hype. They were, for example, the primary justification given (if not believed) for the 2003 invasion of Iraq. Others argue that they drain intellectual and financial resources from more pressing human health needs, and that the risk of accidents overshadows the benefits of the research. Finally, in view of the opprobrium associated with biological weapons, research and development is held to weaken international ties of good will.

The warnings in the *World at Risk* report were repeated by the news media and circulated on blogs. Some commentators scoffed that it was scaremongering, and some members of congress responded that many important preparedness steps had already been taken. There were scattered observations that vaguely declaring a just more than fifty percent chance of ill-defined weapons being used somewhere in the world only established a secure position from which to insist, in the event of an event, that warning

[1] Bob Graham et al., "World at Risk: The Report of the Commission on the Prevention of Wmd Proliferation and Terrorism," (New York2008).

had been given. But the report, despite its hazy phrasing of alarm, recommended a series of specific domestic and international measures that should be enacted to prevent terrorism with chemical, biological, radiological and nuclear weapons. Prominent among the suggestions that related to biology were calls for achieving universal adherence and effective national implementation of two international agreements, the 1972 Biological Weapons Convention (BWC) and the 2004 United Nations Security Council Resolution 1540.

The year before the *World at Risk* WMD report was released, I interned with the Biocriminalization Project at the headquarters of Interpol (the International Criminal Police Organization) in Lyon, France. The project was subsumed under the training-oriented Bioterrorism program, which focused on capacitating law enforcement to deal with biological incidents. Both program thrusts were primarily funded by the Sloan Foundation, as part of the American philanthropy's Selected National Issues program. The biocriminalization sub-project received additional support, at least for translation, from the US Department of State. Fundamentally a legislative endeavor, however, and never a good fit for the police organization, it was subsequently migrated by the lawyer in charge to the Verification Research, Training and Information Centre (VERTIC), an NGO founded in 1986 "to promote effective and efficient verification as a means of ensuring confidence in the implementation of international agreements and intra-national agreements with international involvement."[2] Why "confidence in the implementation" is important will be explored presently.

My work consisted of completing 'legislative surveys.' These were compilations of nations' laws that fulfilled obligations assumed under the BWC, or mandated by UNSCR 1540, for the prohibition and prevention of biological weapons proliferation. I was tasked with Interpol's Spanish, Portuguese, and Catalan-speaking member states. The assignment meant locating and reviewing all the pertinent laws and regulations of those nations, then sorting them into the relevant provisions of a survey template, with 96 discrete analytical criteria. The laws I examined pertained to customs; crimes; export–import; terrorism; money-laundering; international cooperation on judicial and criminal matters; public, animal and plant health; biosafety and biosecurity. The literal text was copied into the survey template, so that nations still in the process of creating their own legislation would have a model to follow, and, ultimately, the national law pertaining to "biocrimes" for every country in the world would be collected in one, consultable place. Yet, the order and conceptual clarity implied by the categories of the template may give the misimpression that the real world was similarly mastered. Biocriminalization convenes much of what is contested about terrorism and crime, emerging science and means of achieving international security.

Biolaws and Biocrimes

The accords I worked with are, or at least aim to be, a step in the creation of international public law: law that applies to the conduct of sovereign states, and some organizations.[3] There is no true authority governing relations between nations that can

[2] "Vertic: About the Centre." http://www.vertic.org/aboutus.asp

[3] For a review of the discussion of legal definitions for "international community", "sources of authority" and the other terms used here, see G M Danilenko, *Law-Making in the International Community*, ed. M. Nijhoff, vol. 15, Developments in International Law, (Boston: Dordrecht, 1993).

autonomously make and enforce decisions, meaning that “law” is a less definite matter than within a country.

> [R]ules have never been perfectly clear. International law has always been a legal system which largely lacked strict formal requirements regarding law-making. As a result, the identification of legally binding rules of conduct among states has always been a difficult task which often depended on extra-legal factors and circumstances.[4]

International law develops and functions through the perception and consensus of the international community. Contingent processes form recursive movements between claims of truth and their jurisdictional enactment. Treaties, conventions, and resolutions are some of the types of documents that are accepted as authoritative.[5] A “source of authority” has two allied meanings: “One sense is related to the origins of the relevant, substantive norms and principles. The other sense is grounded in identifying the actual texts involved in the process.”[6] Authors sometimes try to create a norm by writing a text. Other times, the goal of producing a text is to formalize an already accepted norm. Significantly for biological weapons agreements, the 1899 and 1907 Hague “Laws of War” do both. If an agreement is widely adopted and applied in practice, it produces a recognized legal obligation and creates “custom.” If this happens, in that there is a primary written document, consistent compliance with it, and this is accompanied by a perception of legal obligation, the result is deemed customary international law—the normative process having produced a law that applies to independent nations.[7] The diffusion of the norm occurs in a grassroots fashion through legislative adoption and bureaucratic application.

Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900, by Seth Carus, has become a key reference for definitions. Prefixing “bio-” indicates the use of a biological agent, meaning a pathogen or toxin. Terrorism and crime are differentiated by motive. So, bioterrorism is “the threat or use of biological agents by individuals or groups motivated by political, religious, ecological, or other ideological objectives.” A biocrime, in contrast, has a “criminal” motive.

> Interest in biological agents is not confined to groups with known political agendas. Indeed, most individuals and groups who have used biological agents had

[4] Ibid., xiv.

[5] The legal corpus actively guiding international affairs today has been built from two, largely European traditions—the law of nations (*jus gentium* or natural law), and agreement among nations (*jus inter gentes*) http://www.law.columbia.edu/library/Research_Guides/internat_law/pubint#Definition%20of%20International%20Law

[6] A third source of authority is derivation from general principles common to major world legal systems. Kent McKeever and Last Updated, "Researching Public International Law," *Arthur W. Diamond Law Library Research Guides*(2006), http://www.law.columbia.edu/library/Research_Guides/internat_law/pubint#Definition%20of%20International%20Law.

[7] To be included in this corpus, laws must be “accepted” by the international community of states, and there are several kinds of evidence that can be used to evaluate that acceptance. These include judgments and opinions of national and international judicial and arbitral tribunals, scholarly writings, and purposeful pronouncements by nations that refer to something commonly accepted, intended to become the reference for the law.

> traditional criminal motives. Hence, it is essential to separate the clearly criminal perpetrators from those with political agendas, whether the motive is sectarian, religious, or ecological. The available evidence, in fact, suggests that the vast majority of cases involve criminal motives.[8]

The bioterrorist, he specified, is a non-state actor, thereby sidestepping the issue of nation-states' potential use. While terrorism is sometimes more narrowly defined as an act of violence committed with the intent of effecting political change, Carus wanted to make sure that the acts of a doomsday group seeking to catalyze Armageddon would count. The goal of such groups might not be defined as strictly political, since they do not want to influence governments; they want to completely destroy them, together with most of humanity. Yet these are the groups that are of course most interested in weapons of mass destruction, and so the definition of bioterrorist reasonable needs to encompass them. Carus also wanted to include individuals or groups who choose bioweapons for expediency's sake, rather than purposefully aiming to induce terror through the use of disease. Carus was compiling cases that involved the use of biological agents, and his goal was to provide empirical data that countered what he considered to be apocalyptic visions on the one hand, and the dismissal of a valid threat on the other. These distinctions may seem overly fine, but such is the aim of legal categories. And despite intent, what actually happens in the world escapes their boundaries.

The episode of the globe-trotting, non-compliant tuberculosis carrier, Andrew Speaker, which briefly sparked media attention in 2007, highlights some of the questions about what constitutes a biocrime in a real-world situation. Speaker, a 31-year-old lawyer in the state of Georgia was engaged to be married when he was diagnosed with tuberculosis and began treatment. The strain was identified as multiple-drug-resistant tuberculosis (MDR-TB) and he was informed that he needed to go for special care in Denver. The arrangements, however, would take several weeks, the time in which his wedding and honeymoon in several European countries were scheduled. County officials and his doctor met with him and his family, and, although they said they would prefer he not travel, also stated their belief that he was not a risk to others. Speaker elected to carry out his wedding plans, and flew to Europe, as reports came back to the Center for Disease Control (CDC) that he might have extensively drug resistant tuberculosis (XDR-TB), a more deadly if usually less contagious form. He was contacted in Italy and informed that he should entrust himself to the Italian health authorities, but Speaker decided to return to the US, flew to Prague, then Montreal, and then drove across the border. The border guard received a computer warning when he scanned the passport that the CDC should be contacted, but decided to admit Speaker anyway because he did not look sick.[9] Speaker was quarantined and hospitalized; during treatment it was discovered that his form of tuberculosis was indeed MDR-TB, and thus, unlike XDR-TB, responsive to an aggressive antibiotics regimen.

Keeping someone away from other people is called quarantine when the situation is that of exposure to a disease, and isolation when disease has been confirmed. These are generally combined powers. The problem, as then-CDC Director Julie L. Gerberding testified, was that her authority pertained to "keeping people out and containing them," not

[8] W. Seth Carus, "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents since 1900," (Washington, D.C.: Center for Counterproliferation Research, National Defense University 2001), 3.

[9] "Doctors: Tb Traveler's Diagnosis More Treatable Than Thought," *CNN*, 4 July 2007. http://www.cnn.com/2007/HEALTH/07/03/tb.speaker/index.html

restricting them from leaving the country.[10] Tuberculosis, as one of the most ancient of human diseases, and of great concern in nineteenth- and early twentieth-century Europe and America, comes with a legacy of laws and regulations developed to control it. Yet one carrier wreaked havoc on county, state, federal and inter-nation preparedness plans. Speaker, in the end, was not charged with a crime. However, seven of the people he came into contact with on airplanes filed a civil suit. The sequence of events revealed the ambiguity of biological threats, which do not always have to do with bioweapons, and the resultant inadequacy of "biolaws" and legislative gaps, including the fragility of biomedical expertise, the question of individual versus collective rights when it comes to public health, and cross-border authority.

A crime is an offense prosecutable by the state and punishable by penal law. For *bio*crimes to exist, there must be laws that carve out the difference between permissible and prohibited "biology"-related actions. This is where biocriminalization comes in. Often though, these laws had little to do with scenarios such as Speaker presented. The template I used at Interpol had space instead for a whole range of actions related to the potential malicious use of a biological organism or agent as distinct crimes. The Bioterrorism program description presented its work as follows.

> In many countries, criminal justice systems are constrained by inadequate legal frameworks governing the detection and repression of bio-weapons. Frequently, no law is violated until the disease or biological agent is actually deployed. Law enforcement officers are therefore unable to begin preliminary investigations into the development of such weapons. Without lawswhich criminalise activity relating to bio-weapons, there is no basis for legal assistance or co-operation to prevent their production and transport.[11]

There is, the rationale continues, an urgent need to ensure that countries are adequately prepared for, protected from, and able to deal with would-be bioterrorists. Law enforcement agencies have a crucial role to play, in collaboration with a range of other national and international bodies. The country-by-country database of legislation was intended to underpin the creation of a coherent overlay of laws that made biocrimes a uniform legal reality everywhere in the world, without the need for an (impossible) international law that would make it so.

Disease, intentionally spread or natural, is understood to respect no borders, and hence the database would aid to identify countries with legal gaps. Places without regulation were cause for concern, in that they might provide havens for bioterrorists to set up shop, or the flow of potential weapons materials would go unnoticed and unimpeded. Biolegislation needed to be global because the threat thus conceptualized could come from anywhere, and disease could go anywhere. For a variety of pragmatic and political reasons (discussed later), efforts were focused on getting national legislatures to implement the relevant treaties, rather than strengthening multilateral treaty regimes themselves, through, for example, international verification commissions.

There are two aspects of the idea of biolegislation that I want to bring up. First, practically speaking, the laws criminalize a vast number of acts, such as the transfer of

[10] Alyson M. Palmer, "The Legal Questions Behind the Tb Case," in *law.com* (Incisive Media US Properties, 2007).http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005555593
[11] "The Bioterrorism Threat: Strengthening Law Enforcement," INTERPOL. http://www.interpol.int/Public/BioTerrorism/default.asp

materials or technology. Implicitly or explicitly, they negotiate the “dual-use” dilemma, which is, from the law enforcement perspective, that most acts leading up to an actual attack could be legitimate for research or business purposes. The dilemma is usually framed from a biotechnology perspective though: how can biotechnology both advance towards a producing a brighter human future while taking adequate security measures for the concomitant but unlikely threat of misuse? These share the unacknowledged challenge in the fact that using biolegislation to authorize a law enforcement investigation would, in preventative cases, often hinge on a tenuous gauge of motive. As the Speaker case illustrates, a biological incident may not always be an intended biocrime, which in turn may not relate to bioterrorism. This could be the case in a research-related biological incident, but even more significantly, it is not necessarily simple to discern criminal or ideological intent. Yet, the basis for this new kind of crime often rests on such discernment.

The second issue relates not to preventative investigations, but to how the laws would affect prosecutions. A simple example would be that a federal prosecutor, instead of charging generic homicide or attempted homicide, would charge homicide with a bioweapon in order to request stiffer penalties. This kind of specificity, however, has been of little use for pursing (for example) hate crimes, because it puts a greater burden of proof on the officers and the prosecutors.

Housing the biocriminalization project at Interpol was part of the organization’s move to expand and become a more significant actor on the international scene. Contrary to popular lore, the organization is not an international police force, with arrest powers around the world. Founded in 1923 as mechanized travel (and hence escape) became widely available, “it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.”[12] Perhaps its best-known service is to facilitate communication between law enforcement in different countries about a missing person, a body, a suspected criminal, or a fugitive, thus bypassing diplomatic channels. The color-coded notification service is most frequently mentioned in the press (e.g. “red notices” for arrest with a view to extradition), and these are graded with a required standard of evidence. A less formal “diffusion” for a wanted person can also be used. Interpol Response Teams, which can provide on-the-ground assistance with victim identification after a disaster, or verification of the chemical composition in a drug bust, perhaps come closest to actual police operations. Most of Interpol’s work, though, is serving as an information switchboard.

Ronald K. Noble, the first American Secretary General, was eager to raise the profile and power of the organization. Under him, Interpol entered the computer-age, began “24/7” staffing at headquarters, and strategically selected directions in which to grow. One of these was fighting terrorism and, at least for a while, this included bioterrorism. As Paula Olsiewski, the Sloan Foundation’s Bioterrorism Program Director, told me in an interview, “Ron Noble came to me with Berry Kellman (a US law professor, later a consultant on the Interpol Bioterrorism program), and said he thought bioterrorism was a threat and wanted to work on it. This was the leadership of an international organization saying he thought biosecurity was important, and most people don’t.”[13] At Interpol’s first general assembly after September 11, 2001, Noble announced a reorganization that would focus more resources on terrorism; the creation of a database

[12] "About Interpol," INTERPOL. http://www.interpol.int/public/icpo/default.asp
[13] Interview, July of 2007

for stolen, counterfeit or forged identify documents; and a proposal for making “the issuance of Red Notices for terrorists the highest priority.”[14] By 2005, the Secretary General would declare with drama, “there is no criminal threat with greater potential danger to all countries, regions and people in the world than the threat of bio-terrorism.”[15] Noble maneuvered through tricky terrain with this statement, as he simultaneously defined bioterrorism as 1) a crime 2) of great potential danger to the world’s population.

The definitional gambit—which aimed to depoliticize bioterrorism—was a prerequisite to Interpol’s involvement, because its constitution prohibits “any intervention or activities of a political, military, religious or racial character.” There is the risk, for example, that a country’s request to other nations to arrest someone is a way of defining a political opponent as a criminal. Interpol employs a team of lawyers in the Office of Legal Affairs to scrutinize submissions of red notices and other public actions. Of course perpetrators will generally claim to act for a reason that would place them beyond the reach defined by Interpol’s constitution. So while police officers must attempt to discern motive when investigating a potential terrorist operation, the lawyers must turn to the exact act itself and its verifiable illegality.

Noble’s second declaration, that bioterrorism is at least coequal with other major threats in terms its potential harm usefully encapsulates what skeptics critique and biopreparedness experts claim. “Whether this unhappy Temper was originally raised by the Follies of some People who got Money by it; this is to say, by printing Predictions and Prognostications I know not; but certain it is, Books frighted them terribly," wrote Daniel Defoe in his 1722 *A Journal of the Plague Year*, raising both the specter of fear profiteering and its success, which will be discussed below.[16]

When Interpol sought and received money from the Sloan Foundation (the Bioterrorism Program’s first conference was in March 2005), international terrorism and efforts to counter it were a major focus of US, European, and UN efforts. A “war on terror” approach was imparted largely by US President George W. Bush and UK Prime Minister Tony Blair, but from the outset journalists, academics and other politicians critiqued the war framing. When Gordon Brown took over as the new Prime Minister, in June 2007, he directed that the UK rhetoric change. Terrorism was redefined as a crime problem. In an article on this shift, David Rieff wrote, “Brown’s new home secretary, Jacqui Smith, articulated the basic message. ‘Let us be clear…terrorists are criminals, whose victims come from all walks of life, communities and religions.’”[17] Rieff added, “By emphasizing the criminality of terrorism, Brown effectively changed the terms (and the temperature) of the British debate: he redefined a world historical threat as a manageable danger.” The official US stance, as presented in public pronouncements, gradually began to shift as well. Rhetoric showed the influence, for example, of Australian-born advisor to the US Department of State and military, social scientist David Kilcullen’s vision of a “global counterinsurgency” and moved increasingly towards a fusion of intelligence, policing and military action. Following experience in disrupting organized crime and especially drug cartels, the financial side of terrorist organizations was targeted. Interpol was keen on

[14] Ronald K. Noble, "70th Interpol General Assembly 24-28 September 2001," INTERPOL. http://www.interpol.int/Public/ICPO/speeches/20010924.asp

[15] ———, "Bio-Terrorism Conference 1st Interpol Global Conference, 1-2 March," INTERPOL. http://www.interpol.int/Public/ICPO/speeches/NobleBioTerrorism20050301.asp

[16] Daniel Defoe, *A Journal of the Plague Year*, The World's Classics (Oxford New York: Oxford University Press, 1990 (1722)), 21.

[17] David Rieff, "Policing Terrorism," *New York Times*, 22 July 2007.

fitting itself into this shifting scene. Housing the biocriminalization project was an attempt to position terrorism within the purview of law enforcement, and this fit with the organization's maneuvering to position itself as a global player in counterterrorism.

The 2008 *World at Risk* report brought together discourses and approaches already available, among them those discussed here. It can be examined as an album of certain snapshots of the contemporary—the threat, what needs protection, and how to do it. One picture was of biological weapons, in terrorist hands, which threaten humanity and are best dealt with by a series of domestic and international measures to prevent, and prepare for, an attack. In order to understand how these elements came into place, I will describe the coupled development of some of the significant norms and texts: the 1925 Geneva Protocol, the 1972 Biological Weapons Convention, and United Nations Security Council Resolution 1540.

Binding the Conscience and the Practice of Nations

Signed in Geneva on June 17th, 1925, a succinct one-page "Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare," condemned and foreswore "the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices…by the general opinion of the civilised world." The "High Contracting Parties" agreed "to extend this prohibition to the use of bacteriological methods of warfare" (viruses were not distinguished from bacteria at the time). The Protocol, however, is often described as "toothless," and not very meaningful, because it lacked verification or enforcement mechanisms for impeding the proliferation of either type of weapon.[18] The criticism is of course revisionist in its definition of meaningful, and yet is quite accurate in its assessment that the protocol made no move to keep biological weapons—which in the sense of "a thing designed for inflicting harm"[19] did not yet exist—from coming into existence. What, then, did it aim to do?

Paraphrasing Richard Price on chemical weapons, if it currently seems "a platitude to state that the use of [biological] weapons is a particularly reprehensible and morally unacceptable means of conducting armed conflict," this view dominates because of the success of a normative apparatus that includes the major international agreements.[20] The perspective from which the earlier accords are judged depends on several now-accepted truisms: there is an inherent human aversion to poisons and disease that makes their use as a weapon generically odious,[21] the potential consequences of deployment are too horrific, i.e. they are "weapons of mass destruction,"[22] and that their use would be uncivilized and repugnant.[23]

[18] e.g. Stefan Riedel, "Biological Warfare and Bioterrorism: A Historical Review," *Baylor University Medical Center Proceedings* 17, no. 4 (2004).

[19] *The New Oxford American Dictionary*, (New York: Oxford University Press, 2005).

[20] Richard Price, "A Genealogy of the Chemical Weapons Taboo," *International Oganization* 49, no. 1 (1995).

[21] There are many examples but see Chapter Four Michael Mandelbaum, *The Nuclear Revolution Cambridge* (Cambridge: Cambridge University Press, 1981).

[22] Graham et al., "World at Risk: The Report of the Commission on the Prevention of Wmd Proliferation and Terrorism."

[23] See respectively "Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other

Price points out.

> [N]umerous weapons have provoked cries of moral protest upon their introduction as novel technologies of warfare. However, as examples such as the longbow, crossbow, firearms, explosive shells, and submarines demonstrate, the dominant pattern has been for such moral qualms to disappear over time as these innovations became incorporated into the standard techniques of war.[24]

One entrée to understanding the development of the claims about biological weapons (and up to a certain point, nuclear and chemical weapons share the same path) is to examine the precise elements of the 1925 precedent. There is a list of objects, a regime for governing them, and a rationale for why that presents an implicit moral positioning. Poisons, gases and bacteriological weapons are listed together, and thereby linked. What is prohibited is "use in war." The justification given is the opinion of civilized nations.

Poisons, and later toxins, bridge the biological and the chemical. By the time of the signing of the Protocol, the use of poison was unquestioningly regarded as ignominious. But as Nietzsche notes, "there are no moral phenomena at all, but only a moral interpretation of phenomena,"[25] and the legal history of poison casts doubt on the idea that there is an innately human and, in that sense, timeless taboo against it. There were scattered rejections in Rome and India, but "the formative period for a robust and absolute prohibition against poisonous weapons in Europe appears to have been between the fifteenth and eighteenth centuries."[26] Seventeenth-century legal scholar Grotius explained, and thereby went a long way towards establishing, that while arms could be used in the protection of the king's life, he was humbly vulnerable to poison, unless its use was deterred by "respect for law and fear of disgrace."[27] Correspondingly, any ruler of enough stature had cause to promote a normative injunction against poison. From another angle, poison was delegitimized by its association with women. It was, according to Margaret Hallissy, "an insidious equalizer of strength in the battle of the sexes,"[28] and deemed a less valiant and manly method of attack than openly declared combat. Grouping asphyxiating gases and bacteriological methods of warfare together with poison assisted in tainting them, but poison's own historical course discredits the idea of an inherent moral compunction against their use.

In this era before antibiotics, infectious diseases had very high fatality rates and were certainly feared. By 1921, the French, at least, imagined "liquid cultures loaded onto shells and bombs…detonated to form 'microbial clouds' with great infective power," and

Gases, and of Bacteriological Methods of Warfare," (Geneva1925). and "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction," (London, Moscow and Washington: United Nations, 1972).

[24] He refers to Lawrence, "attempts which have been made to forbid the introduction of new inventions into warfare, or prevent the use of instruments that cause destruction on a large scale, are doomed to failure. Man has always improved his weapons, and always will as long as he has need for them at all" T.J. Lawrence, Principles of International Law, p. 533 quoted in Price, "A Genealogy of the Chemical Weapons Taboo."

[25] Friedrich Wilhelm Nietzsche, *Beyond Good and Evil: Prelude to a Philosophy of the Future*, trans. Walter Kaufmann (New York: Vintage Books, 1966). In Price, "A Genealogy of the Chemical Weapons Taboo."

[26] Price, "A Genealogy of the Chemical Weapons Taboo."

[27] Grotius, Law of War and Peace, Book 3, chap 4, section 15 quoted in Ibid.

[28]Margaret Hallissy, *Venemous Woman* (Westport, Conn: Greenwood Press, 1987)., pp. 5-6, quoted in Price, "A Genealogy of the Chemical Weapons Taboo."

had initiated a formal biological weapons development program.[29] Germ theory was generally accepted by the signing of the Protocol, and some have suggested, from records of an earlier conference, that the representatives intended the prohibition to include purposeful spreading of disease.[30] For all that, it is misleading to equate the conceptualization of biological weapons at the time with contemporary biological "weapons of mass destruction." Such an elision posits that the prohibition of bioweapons was based on a belief that they could pose an existential threat to the human race.[31] In 1925, the example at hand of "bacteriological methods of warfare" was the infection of pack animals intended for the Allies, which combined a variety of underhanded elements, appropriately despicable for an enemy, but not catastrophe.[32] One German naval officer entered the US dressed as a woman, carrying a vial with the highly infectious, but almost exclusively equine disease glanders (*Burkholderia mallei*). His organisms did not survive, although another German agent described infecting horses stabled in New York City:

> The germs were given to me by Captain Hinsch in glass bottles about an inch and a half or two inches long, and three-quarters of an inch in diameter, with a cork stopper. The bottles were usually contained in a round wooden box with a lid that screwed on the top. There was cotton in the top and bottom to protect the bottles from breaking. A piece of steel in the form of a needle with a sharp point was stuck in the underside of the cork, and the steel needle extended down in the liquid where the germs were. We used rubber gloves and would put the germs in the horses by pulling out the stopper and jabbing the horses with the sharp point of the needle that had been down among the germs. We did a good bit of work by walking along the fences that enclosed the horses and jabbing them when they would come up along the fence or lean where we could get at them. We also spread the germs sometimes on their food and in the water that they were drinking. Captain Hinsch gave me the instructions as to where I would find the horses and also gave me bottles of germs and the money. [33]

These low-tech German efforts, reputedly part of a repertoire that also included anthrax, the plague, cholera and wheat fungus, were described as sabotage, an attempt to use germs to disrupt the machine of war fighting. They were perhaps tactically significant (the Germans believed they stopped horse shipments from Argentina) but not a threat to humanity. Some commanders and scientists had qualms about the use of bacteriological disease bombs, but even among those who did not, there was doubt about their battlefield utility. Instead, with the increasing power of airplanes, they were envisioned as a tool of total war, to be used "against reserve troops or against civilians in industries and cities, and against livestock, crops and water supplies".[34]

[29] Jeanne Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism* (New York: Columbia University Press, 2006), 24.

[30] Daniel Feakes, "Global Society and Biological and Chemical Weapons," in *Global Civil Society Yearbook*, ed. Mary Kaldor, Helmut Anheier, and Marlies Glasius (Oxford University Press, 2003), 102.

[31] That fear came into being later, with nuclear weapons. The term "weapons of mass destruction" traces to the United Nation's attempt in the mid-1940s to develop a system for the regulation of armaments under article 26 of the UN charter. Ibid. 96

[32] Carus, "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents since 1900," 69.

[33] Ibid.

[34] Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. 25

Clearly chemical and biological weapons did not produce apocalyptic visions, or even repulsion, for everyone. Proponents advocated in favor of their potential for lessening the destruction caused by conventional weapons. Gas warfare was suggested as “a way to shorten war with overwhelming surprise attacks on the enemy,” and “a humane alternative to high explosives because they avoided battlefield blood and gore.”[35] Some British experts “saw biological weapons as a more humane way not of killing soldiers but of killing civilians already doomed… by aerial attacks with high explosives.”[36] The potential for non-lethal use of these alternative weapons, which is still retained in the use of tear gas for law-enforcement purposes, was also proclaimed in their favor. Although representatives of the United States were involved in developing the 1925 Protocol, advocates of the weapons kept it from being ratified in the US Senate until 1975. One senator in the 1920s justified his objections by contending that if the Protocol passed the US would be constrained

> from using gas against the next savage race with which we find ourselves in war, and would compel us to blow them up, or stab them with bayonets, or riddle them and sprinkle them with shrapnel, or puncture them with machine-gun bullets, instead of blinding them for an hour or so until we could disarm them. That is the 'humanity' that is attempted to be worked out by the Geneva Protocol.[37]

These positions belie the assertion that prohibition was the incontestable march of civilized progress.

The Protocol, plainly, did not come into existence because of now commonplace beliefs or fears about the catastrophic potential or horror of chemical/biological-induced death. It was important, however, in how these claims attained the status of largely unquestioned truths. While the beginning of the pertinent history of biological weapons control is usually located on that June date in Geneva, to paraphrase, John Dewey, this was in many ways already midstream.

Targeting civilians was in fact the real heart of the debate. At the 1874 Brussels Conference on the Laws and Customs of War, more than 50 years before the Protocol, the states represented cemented the anti-poison foundation laid by Grotius, forbidding the “employment of poison or poisoned weapons.”[38] The 1874 declaration did not enter into force but its core proposals became part of the 1899 Regulations Respecting the Laws and Customs of War on Land, signed in The Hague. These also included an agreement to “abstain from the use of projectiles the object of which is the diffusion of asphyxiating or deleterious gases.”[39] Both entered the 1907 Hague Declaration, which went on to become a foundational agreement in the governing of warfare, and one of the first documents of then-developing public international law.[40]

The growth of the chemical industry during the period when these conventions were held brought it to the fore, and concerns were substantialized in discussions of

[35] Ibid. 6

[36] Ibid. 6

[37] Price, "A Genealogy of the Chemical Weapons Taboo." 98

[38] Feakes, "Global Society and Biological and Chemical Weapons," 102.

[39] Ibid.

[40] The 1922 Treaty of Washington (which did not enter into force) introduced the phrase “the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices”, adopted in the Geneva Protocol.

"noxious clouds" as new possible weapons.[41] The specific mention of projectiles diffusing asphyxiating gases is noteworthy, however, because they had not yet been developed. Since, in general, protests against new weapons are lost to their demonstrations of power, it is significant that the gas projectiles were banned even before their advent. Richard Price argues persuasively that this preemptive prohibition was the necessary and truly emergent factor at the 1907 Hague convention. The focus of efforts in the creation of "laws and customs of war" was not on banning technologies, which were viewed as value-neutral, but on constraining their use to combatants. The goal was for war to be civilized, and the defenseless population excluded from its horrors. The first factor in the ban's passage was that asphyxiating bombs were envisioned as being used against defenseless towns with women and children, which made them unsuited to civilized war. (This was long before the destructive bombing with high explosives that later shifted the argument to better and worse ways for civilians to die.) The second factor was that, because they did not yet exist, the proscription was not relevant to any specific party, and little fuss was raised.[42]

The prohibition of use became more important than any inherent attribute of the weapons. Key actors sought to include warfare in a modernizing vogue and the idea of poison gas projectiles gained attention at a crucial juncture. The fact of being singled out then became the basis for future politicization. The successful use of chemical weapons in World War I did not erode the ban, as had historically been the case in the introduction of new technologies. Instead, nations hurled accusations of violations of the Hague Declaration at each other, strengthening its normative status. An ongoing movement towards creating customary international law had been initiated.

The Geneva Protocol tried to "bind alike the conscience and the practice of nations"[43] to produce civilized warfare. Since biological weapons did not really exist yet, although they had been imagined, linking "bacteriological methods" to poisonous and asphyxiating gases was an attempt to extend the solidifying normative injunction against chemical weapons to future biological ones. The technology, however, was not similarly bound. The Protocol was concerned with regulating the conduct of war, not the development of science, or weapons. Asterisks were affixed to the signatures of nations that claimed exceptions to the Protocol's prohibitions. Their own freedom of action was only restrained in relation to other countries that had signed, ratified or acceded to the treaty, and would no longer hold for "any enemy State whose armed forces or whose allies fail to respect the prohibitions." This right to and possible need for retaliation provided a justifying logic for research into and development of biological weapons.

***

Despite the reservations and incomplete ratification among signatories, there was a general lull in bioweapons research after the signing of the Geneva Protocol. Having made a gesture towards "no first use," and given experts' doubts about the potential for precision, governments gave funding priority to arms that would provide battlefield advantage. Only Japan, convinced by military biologist General Ishii Shiro, saw the opportunity to build a stronger hand by developing a type of weapon that most of the rest of the world had forsworn for offensive purposes. The efforts of German science were

[41] Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. 3

[42] Price, "A Genealogy of the Chemical Weapons Taboo."

[43] "Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare."

limited, in part by Adolf Hitler's personal aversion to biological weapons, and in part by its turn to eugenics, and eventually death-camp experiments.[44] Until the mid-1930s, the British avoided the arena. Their entrance was the result of a determined pro-biowarfare campaign on the part of the influential civil servant Maurice Hankey, who served as Secretary to the War Cabinet during World War I, and continued in a long string of secretary, ministry and other bureaucratic positions.[45] When the Second World War was imminent, his personally assembled panel of science advisors was still unconvinced that bioweapons posed a huge threat. They suggested that public health measures were the best defense (in part leading to Britain's system of socialized medicine), and most were unwilling to work on developing offensive capacity. Amid dubious reports of German success in bacteriological aerosolization, Hankey nonetheless advanced a program focused on anthrax, which over the course of a few years produced "cattle cakes," and prototypes for airplane spraying and bombs. He recruited a like-minded bacteriologist to head the secret biological weapons department, one who saw no moral impediment to the research. The bacteriologist, Paul Fildes, believed wholly that a disease such as anthrax was a humane alternative to high explosives:

> Is it any more moral to kill Service men or civilians with HE (High Explosives) than with BW?...It seems clear to me that a substantial majority of the population would conclude that, if they had to put up with war again, they would prefer to face the risks of attack by bacteria than bombardments by HE.[46]

Under his guidance, the department developed bombs, first detonated just off the ground by remote control and then dropped by airplanes from various heights, which successfully killed herds of sheep. The British scientists' own success convinced them (incorrectly) that the Germans must also have made the same breakthroughs. At this juncture, US help was requested, and granted, for industrial manufacture.

Aiding the UK proved the decisive threshold for launching the American bioweapons program, although circumstances were already primed. The Geneva Protocol had linked biological and chemical weapons, and after the Japanese attacks on Pearl Harbor, Secretary of War Henry Stimson decided that on the basis of chemical weapons alone, the United States would not be bound by the not yet-ratified treaty. Compliance, as he saw it, might "through introduction of domestic, political and moral issues, impede our preparation, reduce our potential combat effectiveness and be considered, by our enemies, an indication of National weakness."[47] By winter of 1940, the US was supplying poison gas to the British. The US National Academy of Sciences put together a secret War Bureau of Consultants that, in contrast to the British advisory panel which needed considerable prodding from Hankey, judged that biological weapons could seriously threaten human, animal and plant life, and recommended that the US move forward with offensive and defensive measures.

[44] Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. 42

[45] Ibid. 43

[46] n. 34 reference "PRO, WO188/654 BIO/5293. Fildes Notes on Professor Murray's Memorandum (7 September 1944) in Ibid. quoted in ———, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. 56

[47] Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. 59

Bioweapons research was centered in Maryland, at then-Camp Detrick, and swelled to around 250 buildings, with over 3400 employees. According to Matthew Meselson, a Harvard professor of Biochemistry and Molecular Biology who became a major influence on efforts towards restricting chemical and biological weapons,

> Large-scale production was planned to take place at a plant near Terre Haute, Indiana, built in 1944 for the production of anthrax spore slurry and its filling into bombs equipped with twelve 20,000-gallon fermentors, it was capable of producing fill for 500,000 British-designed 4-pound anthrax bombs a month. Although the United Kingdom had placed a large order for anthrax bombs in 1944 and the plant was ready to go into weapons production by the following summer, the war ended without it having done so.[48]

There was a brief period after the war, from 1945 to 1947, of US government transparency about this biological weapons program, and even though limited to the defensive research that had occurred, the result was too much media attention for the Army's taste.[49]

This was a period in which a fundamental conceptualization of weapons, and hence bioweapons, shifted. The development of the atom bomb forged a new relationship in terms temporal, conceptual and affective, between politics, science, and life. The decision could be made to destroy an entire city, and a single pilot could carry out the order immediately. The two demonstrations of this power, by the United States against Hiroshima on August 6 and Nagasaki on August 9, 1945, entered the public imaginary around the world. Within a couple of years, the size of the weapons had increased to the equivalent of 750 Hiroshimas. Opponents, including Manhattan Project leader Robert J. Oppenheimer, argued that such massive destructive potential, enough to destroy cities the size of Moscow or New York, in effect moved them from battlefield weapons to tools of genocide.[50] A 1995 newspaper article on the Cold War as an age of apocalypse gave this description of the mindset,

> Plutonium—an element created by man and named for the Roman god of the dead—changed the way people thought about time. The future became finite. Student groups in the 1960s came to call themselves "a generation with no future." A certain madness set in. Military planners talked earnestly of "city busting" attacks and casualties in the tens of millions. War, and life on the planet, would be over in a matter of minutes. By the twisted logic of the bomb, fear of that enormous destruction was good. It would so scare the enemy that the cataclysm would never come. Politicians called it "Mutually Assured Destruction.[51]

[48]Matthew Meselson, "Averting the Hostile Exploitation of Biotechnology," *CBW Conventions Bulletin* 48, no. June (2000).

[49] Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. 88

[50] Peter Galison, "Devise and Dissent: The Patriotic, but Unpopular, Career of J. Robert Oppenheimer.," *Slate* 2005.

[51] Brigid Schulte, "As Age of Apocalypse Dawned, So Bloomed a Bunker Mentality " *The Philadelphia Inquirer*, 20 August 1995.

Arsenals were described as existential threats, “enough bombs to kill the world population many times over.”[52]

This sense of threat was not, however, strongly associated with the biological sciences. Biology, and especially the new field of molecular biology that would lead to recombinant DNA techniques, genetic engineering, and eventually contemporary genomics and molecular systematics, was advancing rapidly. The bacteriophage had been isolated during World War I, and the “phage group” of scientists, beginning around 1940, used the bacteria-infecting viruses as its model organism to develop a systematized approach that contributed not just to the understanding of bacteria but also to establishing the field of molecular biology. The 1953 publication of the structure of DNA was one of the more prominent examples of how basic scientific knowledge was multiplying. There were, it is true, black and white educational films and government pamphlets on how to protect against biological warfare attack.[53] Yet, in showing the citizen taking personal health measures, and scientists identifying the unknown bio-assailant, these ultimately reinforced the idea of manageable danger, and positive techno-scientific power. Advances, predominantly, were linked to medicine and the betterment of human life, not mass destruction.[54]

For weapons scientists, however, the power of nuclear weapons changed the stakes, on the ground-level reality of career, prestige, and funding. If nuclear weapons had generated new relationships between bodies and politics, biologists would have to keep up, with their own formula about when, how and how many people it was imaginable to annihilate. Historian Guillemin argues that “Nuclear weapons would set the standard for the next twenty years of biological weapons development, making it imperative for biological warfare scientists to show how pathogens could devastate populations at the same enormous scale.”[55]

According to multiple sources compiled by bioweapons specialist Jonathan Tucker, the Army conducted tests with live agents over the Pacific Ocean in 1965 and 1968.[56] The first demonstrated, with caged monkeys on the decks of anchored tugboats, that an aerosol spray could be infectious over several hundred square miles. The second used a toxin, and the result calculated was that 30 percent of a population spread over 915 square miles would be been incapacitated. “Biological weapons,” the army concluded, “could be employed for strategic, mass-casualty attacks against cities and other population centers.”[57] They were deemed truly, not just hypothetically, weapons of mass destruction. However, development of the weapons tested had taken a considerable investment of time and resources, and another conclusion drawn was that only nation-states with an adequate science, technology and military infrastructure would be able to reproduce the feat. The concern arose that in developing the know-how, the United States was simply making it available for the wrong hands to grasp.

[52] Ibid.

[53] "What You Should Know About Biological Warfare ", (USA: U.S. Federal Civil Defense Administration, 1952).

[54] Francis O. Schmitt, "Contributions of Molecular Biology to Medicine," *Bull N Y Acad Med* 36, no. 11 (1960).

[55] Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*, 91.

[56] Jonathan B. Tucker, "A Farewell to Germs: The U.S. Renunciation of Biological and Toxin Warfare," *International Security* 27, no. 1 (2002).

[57] Ibid. 112

***

On November 25, 1969, President Richard Nixon announced the official end of the US offensive bioweapons program, promising that no more weapons would be developed or created, and all stockpiles would be destroyed. Biological attack, he declared, would have “massive, unpredictable, and potentially uncontrollable consequences. It may produce global epidemics and profoundly affect the health of future generations.” Many saw his announcement as a public-relations stunt. It was certainly a political maneuver that took into account his image domestically and abroad. A series of events had focused negative public attention on chemical and biological weapons, and the resultant domestic and foreign pressure led to congressional requests for an inquiry. Safety was an issue, the making, testing, storing and disposing of the weapons and the feeling was that this, far from contributing to the defense of American citizens, endangered them. Abroad, the idea of the United States’ lack of adherence to what was now customary international law against biological weapons, traceable from the 1925 Geneva Protocol, was seized upon as an asset in Cold War jockeying. Behind the scenes in the White House, though, the secret Pacific Ocean weapons trials, lack of support outside the military, and the absence of a lobbying constituency parallel to that for nuclear and chemical weapons were central to Nixon’s decision.

One shift in the public mood can be traced to an influential television documentary in February of 1969, which reported that a year earlier, 3,000 sheep had died near open-air army testing grounds in Skull Valley, Utah, together with revelations about negligent practices for the disposal of obsolete chemical agents. In July, an accident in Japan exposed that the US army had deployed sarin-filled bombs there without even the knowledge of the White House, and shortly thereafter came news about chemical weapons stockpiles in West Germany. The incidents fed neatly into Soviet Union and allied accusations, begun in 1964, that the US was violating the Geneva Protocol in Vietnam by its use of Agent Orange as a jungle defoliant, and tear gas to force combatants out of tunnels and bunkers into the zone of fire.

With Congress members pressing for an inquiry, and foreign nations raising concerns, Kissinger issued National Security Study Memorandum (NSSM) 59. On behalf of the president, NSSM 59 ordered a thorough review of government programs on chemical and biological weapons. The work was divided among Interdepartmental groups. Members of the Intelligence Community were supposed to assess the programs and capabilities of foreign powers; officials from the office of the Joint Chiefs of Staff and the Bureau of Political Military affairs (the Department of State’s link to the Department of Defense) were to assess practical deployment of chemical and biological weapons; and the legal office of the State Department was to examine “the US position on arms control, including the question of the ratification of the 1925 Geneva Protocol.”[58] The use of these subcommittees was a regular part of the NSSM process, but at the urging of well-connected members of the scientific community, and in recognition of the technical nature of the questions, an additional report on the scientific aspects was requested from experts on the President’s Science Advisory Committee (PSAC).

The PSAC report concluded:

[58] Henry A Kissinger, "National Security Study Memorandum 59," (Washington D.C.: National Security Council, 1969).

> biological weapons were far less reliable in the field and predictable in their military effects than chemical weapons, and had a much shorter shelf life. Moreover, microbial pathogens posed potential long-term hazards because of the possibility that a disease agent could mutate into a more virulent or uncontrollable strain, or could infect wild animals to create persistent foci of disease that would pose an enduring threat to public health.[59]

Their negative pronouncement, as well as that of the State Department, suggested discontinuation of the US program.

In the Department of Defense, however, the two sub-reports that would feed into the final evaluation were in conflict, one largely dismissing the value of biological weapons and the other maintaining that they were "reliable and controllable in the field," without mention of their drawbacks.[60] The Secretary of Defense at this time was Melvin R. Laird, a popular congressman in the House of Representatives, who accepted the secretary appointment but made clear that he only intended to serve one term. He had no allegiance to the agenda of the defense establishment or the Joint Chiefs of Staff personally. Handed these contradictory analyses, he transferred responsibility for the report to a third office. The Office of International Security Affairs commonly staffed the secretary for meetings with the National Security Council and with State. It lacked expertise in chemical and biological weapons, however, and therefore asked permission of the President's Science Advisory Council to draw on their report, which they graciously approved. As a result, the official Department of Defense position, dissented from by the Joint Chief of Staff alone, was virtually identical with the Department of State, and the president was presented with nearly unanimous advice to shut down the program.

The change in US policy opened the way for international negotiations to produce the first significant international legislation addressing biological weapons to be developed since 1925, the 1972 "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction." (BWC)[61] In the time between the two, the conception of the weapons themselves changed fundamentally. In 1925, it was a technology on par with conventional weapons, but like submarines or missiles (about which similar debates occurred), they were fraught with the potential for use against civilians. These weapons were an advance in technology, but a step backwards in movement of mankind. But by 1972, the idea of mutually assured destruction had taken hold. The subtext of the Convention was not early twentieth-century concerns with modernity but Cold War fears. Whereas the object of intervention in 1925 was, literally, the "use in war" of biological weapons, the 1972 Convention prohibited processes of development, production and stockpiling, in order to strengthen "confidence between peoples and the general improvement of the international atmosphere."

In its status as a bellwether lies precisely the problem with the BWC accord. If it were supposed to improve the international atmosphere, that atmosphere would thwart it. Like the Geneva Protocol, the Biological Weapons Convention had no enforcement provisions. The UK, the US and the Soviet governments served as depository parties for the Convention, but this was as much to give themselves seats at the bargaining table as it was an expression of interest in actually ridding the world of biological weapons. Included in the four-page text were provisions for future review of progress on fulfilling the

[59] Tucker, "A Farewell to Germs: The U.S. Renunciation of Biological and Toxin Warfare," 119.

[60] Ibid.: 120.

[61] The US also finally ratified the Geneva Protocol in 1975.

convention's obligations, and meetings to develop a protocol. But the Soviets, apparently convinced that Nixon's renunciation was a subterfuge, in fact intensified their own weapons research. When, during the 1970s, US military intelligence fed them false information about a secret biological and chemical weapons program, the ploy backfired. The Soviets redoubled their efforts, with significant breakthroughs "including development of highly lethal, stable, and persistent formulations of the microbes that cause anthrax, plague, tularemia, and small-pox, as well as advanced delivery systems such as refrigerated warheads for intercontinental ballistic missiles."[62] The illicit Soviet program, now massive in scale by dint of the Americans' goading, and their determination to hide it, would be one of the detriments to the ultimately fruitless negotiations for a verification and enforcement protocol to accompany the BWC.

United Nations Security Council Resolution 1540

UNSCR 1540 was passed in April of 2004, over 30 years after the BWC and nearly 80 years after the Geneva Protocol. While citing and building on those earlier versions of the biothreat, in the new accord, security for the first time moved to center stage as the object of protection. The threat presented was weapons of mass destruction in the hands of "non-State actors." The solution devised was to stop the acquiring, developing, trafficking in or use of nuclear, chemical, or biological weapons and their means of delivery, and related materials. As will be discussed though, a focus on proliferation is no longer adequate if the risk has moved from materials to that of know-how.

Of concern to some, and noteworthy as a procedure in the process of creating customary international law, the resolution was passed by the 15-member Security Council, rather than the General Assembly. Despite this, as a Chapter VII resolution it is technically binding on all members. UNSCR 1540 functions by requiring member nations to pass domestic legislation preventing the proliferation of such weapons and their means of delivery, and establishing controls over precursor materials. It affirmed already existing treaties and encouraged international cooperation in the implementation of the resolution, and subsequent verification. Much of this legislation was what I collected for the biocriminalization template at Interpol.

Despite the cooperative rhetoric of the text, UNSCR 1540 was severely criticized. The resolution was viewed as having been pushed through by the United States to support an at least partially discredited antiterrorism agenda. Negotiated principally by the permanent five members in the Security Council, the great majority of states were excluded from its development. Complaints arose about the Security Council acting as a global legislator. The language of 1540 was also ambiguous about disarmament and nonproliferation, adding fuel to long-smoldering complaints about an international double standard that strengthened the position of those who were already armed and impeded the pacific technological development of those who were not. In many ways, these paralleled the problems that had arisen in the development a protocol for the Biological Weapons Convention, an attempt shelved in the summer of 2001.[63]

[62] Tucker, "A Farewell to Germs: The U.S. Renunciation of Biological and Toxin Warfare." 144

[63] Kenneth D. Ward, "The Bwc Protocol: Mandate for Failure " *Nonproliferation Review* Summer(2004).

Historian Susan Wright has detailed extensively how biological weapons came to be linked with terrorism in such a way that their use became a matter of not if, but when and where. According to former National Security Council senior staff members, Wright reports, before 9/11 "terrorism was perceived as 'a nuisance to be attended to, not a strategic threat.''"[64] The 1993 World Trade Center bombings were considered the work of unstable fanatics rather than the brazen act of an organized terrorist network that demanded immediate retaliation and countering. That first WTC attack was not, according to the staff members Wright quotes, ''the kind of issue to provide an organizing principle for America's dealings with the world.''[65] Terrorism was thought of as a demand for media attention on a desired cause. Killing massive numbers of people would offend rather than convert, and ultimately turn people away from joining or even supporting. Wright attributes the change in relation to biological threats to a small group of people with strong convictions. These individuals had the connections to make their concerns matter. In a deluge of detail, she describes how they became convinced that the threat from bioterrorism was real, in what ways their campaign was also self-serving, and the manner in which they disseminated their beliefs.

As one among many other elements, she points to Richard Preston's bioterrorism novel *The Cobra Effect* as an influence on then-president William J. Clinton. Wright identifies a subsequent 1998 Clinton address in which "the threats of the twenty-first century would come from connections between 'rogue' states and terrorists and from the real risks that chemical and biological weapons would be transferred from the former to the latter."[66] Another historian of science, Nicholas King, has argued that the book crystallized the American discourse on bioterrorism, which "is both a legitimate response to a nascent threat and a subterranean dialogue shaped by peculiarly American ambitions and anxieties about social change in a globalizing era."[67] Bioterrorism has become, according to him, "a focal point of American anxieties about globalization, demonstrating the difficulty of maintaining security amidst global transportation and information networks."[68] In Preston's novel, "these bioterrorism experts treaded a fine line between speculation and analysis, constructing fictional scenarios in order to develop medical and political responses to future events."[69] The worst-case scenarios in the novel were no different that those developed by real world experts, in disaster preparation, disease modeling and asymmetrical warfare.

A body of security and social science literature has explored this construction of bioterrorism, poking at the speculative seams of such scenarios. At one extreme is the claim that bioterrorism is predominantly a representation of social insecurity, and its significance "lies in the fear that it generates, `threat' in this context constituting not just a physical manifestation of impending danger but also a reflection of a subjective vulnerability derived from a fear of an eventuality that cannot be predicted, identified or controlled."[70] Melinda Cooper has focused on how and why bioterrorism, on her view "is

[64] Susan Wright, "Terrorists and Biological Weapons: Forging the Linkage in the Clinton Administration," *Politics and the Life Sciences* 25, no. 1-2 (2007): 66.
[65] Ibid.
[66] Ibid.: 86.
[67] Nicholas B. King, "Dangerous Fragments," *Grey Room* Spring, no. 7 (2002): 73.
[68] King Nicholas B, "The Influence of Anxiety: September 11th, Bioterrorism, and American Public Health," *Journal of the History of Medicine* October, no. 58 (2003): 439.
[69] King, "Dangerous Fragments," 73.
[70] Sonja Kittelsen, "Conceptualizing Biorisk: Dread Risk and the Threat of Bioterrorism in Europe," *Security Dialogue* 40, no. 1 (2009).

becoming the paradigmatic threat of US defense policy, the virtual characteristically emergent event around which it is reorganizing its whole vision of warfare."[71] She surmises that an understanding of biological knowledge as emergent and unpredictable cannot be dealt with by previous probability and risk approaches, and instead is easily tied to a military doctrine of preemption, which deals with the uncertainty of potential catastrophe by turning it instead into a future of its choosing, or in Deleuzian terms, actualizing it.

Others, such as longtime bioweapons specialist Milton Leitenberg, emphasize the incongruence of devoting vast resources to a threat that, in terms of historical antecedents and probability pales next to poverty, infectious disease or global warming.[72] Richard Danzig, lawyer, former Secretary of the Navy, and one the individuals Wright indicates as shaping the current biothreats framing, lays out the reasons for his position and activism. While "biological weapons currently pose a threat somewhere between conventional explosives and nuclear weapons, the "ability to 'reload' and attack repeatedly with biological weapons is likely to be very attractive to terrorists. It will give them a supreme opportunity to hold us hostage."[73] He emphasizes that skills to produce biological weapons are proliferating, so that "Only a thin wall of terrorist ignorance and inexperience now protects us." Finally, "there is a frightening category of biological weapons—those that do not exist in nature" but could be engineered in the future. This last is the main concern of molecular biologist Roger Brent, which he expressed to me in an ongoing correspondence on the subject as, "The thing to worry about is an attack with a contagious disease. The equivalent of a "strategic" attack with nuclear weapons. That kills zillions of people. All else is less important."

The feasibility of this last assertion forms a divide between biosecurity experts. Wright observes of the late 1990s period, "Many people understood at this point that producing bioweapons with the capacity for mass destruction would not be readily accomplished by a few people operating alone in a basement laboratory. This required technical expertise and substantial support."[74] This position is still maintained by many in both policy and the social sciences. At variance with it, writing in 2005, Brent declared "the history of the use of biological weapons in war and of the 20th century germ war programs is largely irrelevant to the current strategic situation." He elaborated in his testimony before the US House Homeland Security Subcommittee on Prevention of Nuclear and Biological Attack that same year:

> Just as with computers, revolutionary changes sustained over time have revolutionary consequences, and much of the first part of this century will reflect these changes breaking surface to impact human affairs…
>
> …there are tens of thousands of people worldwide who can now engineer drug resistant bacteria, and thousands with the ability to remake a virus like SARS, or

[71] Melinda Cooper, "Pre-Empting Emergence: The Biological Turn in the War on Terror," *Theory, Culture & Society* 23, no. 4 (2006).
[72] Milton Leitenberg, "Bioterrorism, Hyped," *Los Angeles Times*, 17 February 2006; ———, *Assessing the Biological Weapons and Bioterrorism Threat* (Carlisle, PA: Strategic Studies Intitute, 2005).
[73] Richard Danzig, "Proliferation of Biological Weapons into Terrorist Hands," *The Challenge of Proliferation* (2006).
[74] Wright, "Terrorists and Biological Weapons: Forging the Linkage in the Clinton Administration," 87.

> perform other engineering tasks too numerous to mention. Their numbers will only grow, so I would not be surprised if, by 2010, there were more than 100,000 people worldwide who had the knowledge and access to the lab equipment they would need to use to make, say, anthrax resistant to Ciproflaxin. Since the breadth of dissemination of this technical knowledge base will only increase, if you assume that some of these people may be motivated to undertake these tasks, then you have to look at the next decades are a time of great and increasing risk. If you further assume that some individuals or groups may be motivated to use relatively crude deployment methods, at the limit including infecting themselves and spreading the disease by human transmission, then you have to figure that the increase in the risk is higher still. These projects could be carried out by individuals or small groups of people; there would be no need to recreate the Cold War programs of the nation states.[75]

Kathleen Vogel, a chemist who has worked in science policy and academia, discusses what she characterized as the “biotech revolution model.” She is not concerned with proving or disproving the threat, although she suggests that it doesn’t yet exist in the way that concerns Brent. Rather she examines how framing biosecurity directs and limits the way it is approached. “Instead of a revolutionary model,” she argues, “empirical studies suggest that as biotechnology moves from the scientific bench to a more applied setting, it follows a well-established historical pattern of slow and incremental change and diffusion consistent with other major technologies.”[76] “[W]ell-established laboratory practices and techniques,” according to her research, are what made possible the experiments that are often used as examples of impending infectious danger (synthesis of the poliovirus and phiX bacteriophage synthesis). Countering the notion of the infinite possibility and proliferation of technoscience, she maintains that there is a difference between tacit and explicit knowledge and this could become a focus of preventative measures.[77] She concludes, “the current dominant biosecurity frame takes away policy attention from other important considerations for assessing the threat from biotechnologies and designing appropriate policy responses.”[78]

Brent’s opinion is in some ways in agreement with Vogel’s. “Most of the helpful steps are not technical but social,” he wrote me in another exchange, but he is less assured about the social impediments to the transmission of tacit knowledge. The situation, as he views it, can be framed in analogy with advances in computing, hackers and computer viruses:

> There is a decentralized, Moore’s law type, revolution in biological understanding and capability going on worldwide for more than half a century. In some cases, biotechnology is advancing faster than computer technology. For example, the density of components on computer chips continues to double every 18 months—while certain abilities to read and write DNA double more like every 12 months. [79]

[75] Roger Brent, "Testimony of Roger Brent, Phd to the U.S. House Homeland Security Committee, Subcommittee on Prevention of Nuclear and Biological Attack " (Washington, DC2005).

[76] Kathleen Vogel, "Framing Biosecurity: An Alternative to the Biotech Revolution Model?," *Science and Public policy* 35, no. 1 (2008): 50.

[77] Ibid.

[78] Ibid.

[79] Brent, "Testimony of Roger Brent, Phd to the U.S. House Homeland Security Committee, Subcommittee on Prevention of Nuclear and Biological Attack ".

The implication is that if a lone computer hacker can produce a devastating digital virus, then a solitary mad scientist could produce a catastrophic organic virus. Little institutional framework would be necessary. To his mind even more dangerous is the possibility of a biohacker community within which a veneer of renegade chic would be associated with clever, subversive destruction. Vogel proposes that biosecurity be approached with a “material and informational focus,” intervening in “more qualitative aspects of biotechnology, such development of laboratory skills and disciplines, organizational communities of scientific practice, contingency and complexity of laboratory work, and so forth.”[80] Brent concentrates more on creating a moral climate among researchers, such that the potential for harm is fully and negatively understood. He promotes the adoption of a code of conduct and ethics oath for biological scientists, with the goal of constituting an alternative community, which he views in moral terms, and instilling in researchers an internal injunction against malevolent use of biology.

What an oath might do pragmatically would be to raise awareness that someone might want to do harm. It can therefore have the effect of increasing vigilance, and creating a climate in which whistleblowers are inclined to come forward. The problem with tools such as codes and oaths is that ethical behavior, understood as intrinsically a form of self-responsibility, cannot be imposed. The people who would take the oath seriously do not need it. They already work consistently to emerge from their self-imposed immaturity. The risk of a mandatory oath is that it would be taken as an empty infliction of authority, so that the sense of self-responsibility, which is in fact the goal, is undermined. Researchers would not necessarily do harm, but the oath, if it did not inspire reflection, would similarly leave unaffected their decisions or behavior. This can cheapen the very values sought, as indicated by the history of the California State loyalty oath,[81] or even the US Pledge of Allegiance.

Deterrence

A year to the day of the 2001 terrorist attacks on the US, then-President George W. Bush signed into place a new US National Security Strategy. The assumption in the strategy was that “traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents.”[82] Over the course of the next few years, however, thinking seemed to change. The 2006 National Strategy for Combating Terrorism concluded: “A new deterrence calculus combines the need to deter terrorists and supporters from contemplating a WMD attack and, failing that, to dissuade them from actually conducting an attack.”[83]

Breaking down this statement helps identify something important. Deterring terrorists from “contemplating a WMD attack” refers not to operational impediments, which falls under dissuasion from “actually conducting” it, but suggests that a biological weapons attack should be “unthinkable.” It should not be an option under consideration because it would be counterproductive. This is an important conceptual and strategic shift. The word

[80] Vogel, "Framing Biosecurity: An Alternative to the Biotech Revolution Model?."

[81] "The Loyalty Oath Controversy, University of California 1949-1951," (Berkeley: Regents of the University of California, 2006).

[82] Eric Schmitt and Thom Shanker, "U.S. Adapts Cold-War Idea to Fight Terrorists," *International Herald Tribune*, Tuesday, 18 March 2008.

[83] "National Strategy for Combating Terrorism," ed. Homeland Security (Washington DC: White House, 2006), 14.

itself, “deter,” appeared in the mid-sixteenth century, coming literally from the latin *deterrere*, joining *de-* “away from” + *terrere* “to frighten.”

While “frightening away” is most often associated with punishment, it can also indicate more subtly the effects of stigmatization, or changing the accepted norm. In legal terms:

> Criminal law is not only a price tariff but also an expression of society's disapproval of forbidden behavior, a fact influencing citizens in various ways. Most people have a certain respect for formal law as such. Moreover, the criminalization of a certain type of behavior may work as a moral eye-opener, making people realize the socially harmful character of the act ("the law as a teacher of right and wrong"). The moral condemnation expressed through the criminal law may also affect the moral attitudes of the individual in a less reflective way. Various labels are used to characterize these effects: the moral, the educative, the socializing, the attitude-shaping, or the norm-strengthening influence of the law. From the legislator's perspective, the creation of moral inhibitions is of greater value than mere deterrence, because the former may work even in situations in which a person need not fear detection and punishment. In the Scandinavian countries and Germany the moral component in general prevention is considered to be essential. For the moral effect of criminal law the perceived legitimacy of the system, rooted in the application of principles of justice, proportionality and fairness, are regarded as more important than severity of sentences.[84]

“New,” however, is a relative term. Deterrence as retaliation is described as outdated, but the replacement in many places is “consequence mitigation,”[85] or “deterrence by denial—the ability to defeat, defend against, and operate in the context of WMD and, if needed, overcome the effects of WMD use.”[86] In keeping with this approach, the former Center for Deterrence of Biowarfare became the Center for Health Hazards Preparedness (CHHP). Preparedness became understood in some circles as the best form of deterrence, and in fact synonymous with it. The acting director of the National Counterterrorism Center, Michael Leiter, at the time said, "What we've developed since 9/11, in six or seven years, is a better understanding of the support that is necessary for terrorists, the network which provides that support, whether it's financial or material or expertise.” One form of deterrence is certainly to target those networks. "We've now begun to develop more sophisticated thoughts about deterrence looking at each one of those," Leiter said in an interview. "Terrorists don't operate in a vacuum."[87]

> Leiter points to the fact that terrorism is not random violence. Unless the terrorist identity is constructed purely on opposition, and violence is intended to strengthen internal cohesion, a group has two intended audiences: victims and observers. Observers can identify with either the terrorist or the victims, and thus be either

[84] Johannes Adenaes, "Deterrence - the Concept. A Historical Perspective, Empirical and Ethical Questions, General Deterrence: Myth or Reality?," in *Law Library Crime and Justice Vol 2*.

[85] Barbara Honegger, " Nps News Profile Nps Prof Publishes Groundbreaking Book on Bioweapons
Monday, November 17, 2008. National Security Affairs Assistant Professor Anne L. Clunan)," *News, Center for Contemporary Conflict, Naval Postgraduate School* 2008.

[86] Jason D. Ellis, "The Best Defense: Counterproliferation and U.S. National Security," *Washington Quarterly* 26, no. 2 (2003): 129.

[87] Schmitt and Shanker, "U.S. Adapts Cold-War Idea to Fight Terrorists."

> galvanized to join the cause or repulsed. The new deterrence focuses on those who might previously have been inspired, aiming to change the audience so that the act of terror is viewed negatively. This version of soft propaganda

, even covert, is not new either, and has antecedents in war efforts, marketing and political campaigns. What is emergent in the scenario is only the recognition that it could be effective against terrorism at a grass roots level. Described in a 2008 *New York Times* article,

> American officials have spent the last several years trying to identify other types of "territory" that extremists hold dear, and they say they believe that one important aspect may be the terrorists' reputation and credibility with Muslims. It aims to mute Al Qaeda's message, turn the jihadi movement's own weaknesses against it and illuminate Al Qaeda's errors whenever possible.[88]

This sense of deterrence is fits with the law and law enforcement understanding of the goals of criminalization. A narcotics veteran I interviewed once used a similar logic to explain the role of drug enforcement, “It is, at least in part, stigmatization.”

The deterrence of which Leiter spoke works on changing the milieu within which terrorism has effect. The argument is made, for example, that by engaging in torture the United States delegitimized itself. In this same milieu, the U.S. must now reestablish credibility. Evidence in favor of the power of a moral framework includes the refusal of Indian Muslims to bury the 2008 Mumbai attackers. M.J. Akbar, the Indian-Muslim editor of *Covert*, an Indian investigative journal, declared:

> Terrorism has no place in Islamic doctrine. The Koranic term for the killing of innocents is ‘fasad.’ Terrorists are fasadis, not jihadis. In a beautiful verse, the Koran says that the killing of an innocent is akin to slaying the whole community. Since the ... terrorists were neither Indian nor true Muslims, they had no right to an Islamic burial in an Indian Muslim cemetery.[89]

He was quoted in an *New York Times* op-ed by Thomas Friedman who added, “The only effective way to stop this trend is for “the village” — the Muslim community itself — to say “no more.” When a culture and a faith community delegitimizes this kind of behavior, openly, loudly and consistently, it is more important than metal detectors or extra police. Religion and culture are the most important sources of restraint in a society.” [90]

Tracking the Threat

Returning to the *World at Risk* report and its conceptualization of the threat: the claims and beliefs about bioweapons encapsulated in the agreements have become so effectively normalized that it requires a certain effort to see the extent to which they present contingent conceptualizations. The contemporary framing of the problem and attendant focus on non-proliferation was expressed in the words of the WMD Commission:

[88] Ibid.
[89] Thomas L. Friedman, "No Way, No How, Not Here," *New York Times*, 17 February 2009.
[90] Ibid.

> The proliferation of these weapons increases the risk that they may be used in a terrorist attack in two ways. First, it increases the number of states that will be in a position either to use the weapons themselves or to transfer materials and know-how to those who might use WMD against us. The more proliferation that occurs, the greater the risk of additional proliferation, as nations that have to this point declined to acquire nuclear weapons will believe it necessary to counter their neighbors who have developed those capabilities. Second, it increases the prospect that these weapons will be poorly secured and thus may be stolen by terrorists or by others who intend to sell them to those who would do us harm.

Counterproliferation, like counterterrorism, denotes proactive measures. There is a distinction made between the antiterrorism and counterterrorism in the military that seems to have drifted into other realms, although the news media generally conflates them in favor of the term counterterrorism. Antiterrorism is used by the military to refer to preventative efforts (e.g. erecting a barrier outside of an airport to prevent bomb attacks) or neutralizing, "preparedness" actions (e.g. vaccines for a bioterrorism attack). Counterterrorism in contrast is understood to be pro-active, such as operations in pursuit of terrorists. Thus when Jason Ellis, research professor at the Center for Counterproliferation Research, National Defense University, writes "counterproliferation—defined by the secretary of defense as the 'full range of military preparations and activities to reduce, and protect against, the threat posed by nuclear, biological, and chemical weapons and their associated delivery means'—is of central importance,"[91] this is code for proactive measures. Proactive, in turn, can mean preemptive, including strikes to destroy physical locations, but also controlling materials, as well as gathering operational intelligence about acts of terrorism, or investigating financial networks.

Despite the bravado of counterproliferation thus expounded, it still suggests the containment of something, such as knowledge, which in the context of biology should rather be considered uncontainable. Marc Ostfield, US State Department advisor on bioterrorism, biodefense and health security, argues that counterproliferation is not only the wrong word, but the wrong approach: the necessary bioscientfic skills have already proliferated. "Control" is the wrong conceptualization and wrong tactic. He returns us instead to deterrence. The debate, ultimately, is muddled by overlapping but incommensurate analytical frames.

Andrew Lakoff and Stephen Collier have together developed a schema for thinking through types of collective security. Different types can be analyzed as having: an object, a moment of articulation, a normative rationality, a type of threat, an exemplary form of knowledge and a basic operation.[92] In these terms, international security can be thought of as the converse of sovereign state security: the unit, or object is not the state but more exactly the stable relations between states. The moment of articulation can be traced to the conventions and treaties relating to warfare around the turn of the twentieth century, and then the League of Nations, followed by the United Nations. These were organizations with the power to produce laws that abstractly, would govern the community of nations. The operation that Lakoff and Collier pinpoint for sovereign state security is deterrence and defense against enemies. For international security qua stability, the principal operation has been the passage of treaties and legislation that nations are then obliged to fulfill domestically. Treaties and legislation have become the major

[91] Ellis, "The Best Defense: Counterproliferation and U.S. National Security," 116.
[92] Andrew Lakoff, "The Generic Threat, or How We Became Unprepared," *Cultural Anthropology* 23, no. 3 (2008): 403.

governmental – but not scientific – strategy for dealing with biological threats identified as international, supported by watchdog NGOs that document, critique, agitate and in some arenas assist in the implementation and verification of the promises between countries.

One point to notice is the way that biotechnological prowess and the terrorist are understood. As mentioned, the conventional wisdom long held that a technology transfer from a rogue state would be necessary for a truly devastating biological attack. In Preston's *The Cobra Effect*, Clinton's address and even UNSCR 1540, with its focus on nonproliferation, the idea that bioweapons could only be developed by a state power still prevailed. One stroke of erasure of this belief, at least in some scientific and policy circles, has come from advances in the biological sciences. The threat is reframed in terms of knowledge and skills, removing the need for a state actor to transfer either the weapons or the know-how. Another stroke of erasure was the gradual acceptance, which came only after the 9/11 Commission Report, that a non-state organization such as al-Qaeda was organized and strong enough to commit a major act of terrorism without direct state support. Wright, among others, discusses views of terrorism experts that debates on bioweapons tend to ignore the history of terrorist actions and intent. RAND Corporation expert Brian Jenkins asserted in 1999, "Threat assessment based on infinite vulnerabilities, conjured foes, worst-case scenarios, and the wrath of our children can degenerate into a fact-free scaffold of anxieties and arguments—dramatic, emotionally powerful, compelling, but analytically feeble.'' Although less than 3000 people were killed on September 11, 2001, in the grandiosity of the act, it became conceivable that a terrorist goal would be mass death. By this interpretation, rather than numbers, 9/11 altered the previous expert opinion that, ''Terrorists want a lot of people watching, not a lot of people dead."[93] The 9/11 Commission report also opened the doors to scenario-imagining in another way. One of their findings was that analysts had lacked imagination. Referring to the US government just before the Japanese attack of 6 December 1941, Thomas C. Schelling observed: "There is a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered seriously looks strange; what looks strange is thought improbable; what is improbable need not be considered seriously."[94] The Commission's emphasis on imagination not only liberated thinkers from the need to consider only the probable, it pushed for thinking the unthinkable, and bioterrorism presented itself as that unlikely but possible candidate for the position of favored threat.

Jez Littlewood, in an assessment for the Weapons of Mass Destruction Commission (WMDC), attempted to reform the terminology of biological threats at its core: "The key issue," he affirmed, "is the 'problem' and not the 'threat'."[95] What Littlewood meant is that there have been a number of versions over time, but the fact of threat has

[93] Brian Jenkins, ''International Terrorism: A New Mode of Conflict,'' in David Carlton and Carlo Schaerf, eds., International Terrorism and World Security (London: Croon Helm, 1975), p. 15. Quoted in Wright, "Terrorists and Biological Weapons: Forging the Linkage in the Clinton Administration," 67.

[94] Thomas C. Schelling, "Foreword," in *Pearl Harbor: Warning and Decision* (Stanford: Sanford University Press, 1962).

[95] Jez Littlewood, "Managing the Biological Weapons Problem: From the Individual to the International," in *Weapons of Mass Destruction Commission (WMDC) Papers and Studies* (2004). ii The Commission he was writing for was proposed by the United Nations and established by the Swedish Government. Members were selected by former Iraq WMD inspector Hans Blix from "a broad geographical and political base". Its mandate is to develop "proposals aimed at the greatest possible reduction of the dangers of weapons of mass destruction, including both short-term and long-term approaches and both non-proliferation and disarmament aspects".

remained constant. This continuity should be the focus, not the weapons themselves or a weapons convention, disarmament, or bioterrorism. The biological weapons problem is "a spectrum of risks and threats involving biological weapons" but "this spectrum is itself only part of a number of risks related to biological organisms and/or the life sciences, such as genetically modified organisms, synthetic biology, accidents involving pathogens, natural outbreaks of disease, etc."[96] As a result, "the biological weapons problem is one to be 'managed'; not solved."[97] This is where the normative effect of the international accords comes in. Both the 1925 Protocol and the 1972 Convention are concerned with acceptable practices of war. Nixon's renunciation, in the midst of Vietnam, was specifically about total war.

There is debate among historians about how far back the concept of total warfare can be traced and still retain enough specificity to refer to and be useful for describing conflicts today. The Peloponnesian war is sometimes labeled the first documented "total war," in comparison to what are described as more ritualistic, earlier Greek wars, fought exclusively between soldiers. The key differences were that the civilian population was deemed a legitimate target and that the economies of the city-states were mobilized in function of the war. Other military historians argue that complete redirection of resources only becomes possible after the industrial revolution, or that total warfare appears with the advent of aerial bombings, which diminished the importance of the battle line, and made vulnerable populations otherwise removed from battle. The register of the debate among historians is technical, not conceptual. It does not address a notion of the interpellation of a people when presented with war—that when a country goes to war, a citizen may support or reject the mobilization but regardless is compelled to respond. Instead, the historians generally differ in which real world war should serve as the ideal type, in relation to which other wars are categorized. They leave aside the possibility of considering at what point, or via what means fundamental relations between politics and the population shifted.[98]

That relationship is crucial to the imaginary within with biological weapons came to be developed, produced and eventually prohibited, although not abandoned. The impetus to civilize war by limiting it to soldiers vied with and often lost to the goal of victory. The history of biological weapons development is tied to the rise and fall of that impetus rather than its success or failure. Nuclear weapons had introduced the idea of existential threat but it would take the advances in genomic science for biological weapons to enter this space as well. Even if the concept of total war is reserved for industrial-age conflicts, and the definition of biological weapons limited to scientifically developed military projects, the purposeful use of disease indicates a willingness to assault the general population. In the latest incarnation of bioterrorism, technoscience became both the problem of engineered germs, and the solution of a system of technological surveillance, improved disease detection and identification, and flexible vaccines that can go into rapid production.

International legislation more generally can be understood as a political and normative framework through which certain kinds of threats have been made accessible

[96] Ibid.

[97] Ibid.

[98] As Roger Chickering, historian of European history, and especially German empire, writes, "Defining the Second World War as the paradigmatic instance of total war has important methodological ramifications". Roger Chickering, Stig Förster, and Bernd Greiner, eds., *A World at Total War: Global Conflict and the Politics of Destruction, 1937–1945*, Publications of the German Historical Institute (Cambridge: Cambridge University Press,2005).

to technical intervention. Terrorism and total war share the characteristics of targeting civilians and disregard for other, “civilized” conventions of war. Such legislation moves slowly and tends to build on previous models, so that the nonproliferation models are based on an idea of the biological weapons threat that dates to an era when terrorism was most commonly coupled with “state-sponsored” and weapons needed the support of a state apparatus to be developed. Nonetheless, this legislation is a necessary if not sufficient, step.

The development and use of each kind of specified weapon in UNSCR 1540 is regulated by previous agreements—the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention and the Biological and Toxin Weapons Convention, and tracked, in the case of the first two, by the International Atomic Energy Agency and the Organization for the Prohibition of Chemical Weapons. Biological weapons, notably, lack a parallel implementation and verification organization. Even with a treaty or resolution in place, implementation is a separate, and often interminable, process. Littlewood, whose argument is representative of a range of disarmament NGOs, makes the case for pursuing this course nonetheless.

> If the BWC continues to remain peripheral to efforts to counter biological weapons—as it currently does—its purpose and function will be thrown further into doubt. That will lead only to erosion of the law underpinning biological disarmament, the law and the norm against the use of such weapons, and the moral revulsion against them (which itself is routinely cited but rarely given any meaning).[99]

Nonproliferation accords are unlikely to control the flow of knowledge and materials used to develop weapons, but that does not mean they are useless. What they do, at very high level, is create a moral climate. Their relevance comes from their normative power.

[99] Littlewood, "Managing the Biological Weapons Problem: From the Individual to the International."

Chapter Five. Events and Failures

From the moment it became clear—as a second plane struck the World Trade Center— that a non-natural disaster was unfolding in the United States, two phrases spontaneously shaped the experience: Pearl Harbor and intelligence failure.[1] Terrorism was invoked descriptively, but the connections to World War II and intelligence were the first interpretations. They appeared immediately, unprompted, in television and radio commentary across the nation. Both stuck. Having done so, they gave form to the event of 9/11, and ultimately influenced responses to it. The impression of rupture of that day would become part of the story, the narrative hub of causes and effects.

Gilles Deleuze, in early work and later with collaborator Guattari, proposed an influential concept of the event, detailing its nature, temporality and actualization. Their identification and specification of an "event" is a useful analytic for evaluating what would become 9/11.[2] Drawing on the Stoics, Deleuze defined "bodies" as things with "tensions, physical qualities, actions and passions."[3] At a given point in time, bodies are in a static relationship with each other. The relationship changes when bodies interact, producing an "event." For example, "a knife in flesh" is a relationship of two bodies; "being cut" is the effect, and an event. Within their framework, the effect/event is incorporeal, and events do not cause other events. "Incorporeal effects are never themselves causes in relation to each other,"[4] although Deleuze allowed that they may be "quasi-causes."

"Actualization" is Deleuze and Guattari's word for describing the event "embodied in a state of affairs, an individual, or a person, the moment we designate by saying 'here, the moment has come.'"[5] Within this period, "The future and the past of the event are only evaluated with respect to this definitive present."[6] "On the other hand," Deleuze notes, "there is the future and past of the event, considered in itself… free of the limitations of a state of affairs."[7] For Deleuze, these are two distinct kinds of time. In the former, an event takes specific, defined form; in the latter, it is a "pure event," "the expressed of statements and the 'sense' of what happens."[8] The pure event does not exist outside of human cognizance. It is "sense itself," and requires description.[9] Pertinent to the events of to be discussed below, Paul Patton writes, "language use is not primarily the communication of information but a matter of acting in or upon the world: event attributions do not simply describe or report pre-existing events, they help to actualize particular events in the social

[1] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 191.Rosenberg writes, "By this term, I mean those evocative rhetorical conventions that come to stand, as a kind of shorthand, for larger stories and meanings".

[2] Paul Patton, "The World Seen from Within: Deleuze and the Philosophy of Events," *Theory and Event* 1, no. 1 (1997), http://muse.jhu.edu/journals/theory_and_event/v001/1.1patton.html.

[3] Gilles Deleuze, *The Logic of Sense* trans. Mark Lester and Charles Stivale (New York: Columbia University Press, 1990), 4.

[4] Ibid., 6. "'quasi-causes' following laws which perhaps express in each case the relative unity or mixture of bodies on which they depend for their real causes."

[5] Ibid., 172.

[6] Ibid.

[7] Ibid. He names these Chronos and Aion: "Whereas Chronos expressed the action of bodies and the creation of corporeal qualities, Aion is the locus of incorporeal events" p. 165

[8] Patton, "The World Seen from Within: Deleuze and the Philosophy of Events."

[9] Deleuze, *The Logic of Sense*

field. That is why politics frequently takes the form of struggle over the appropriate description of events."[10]

It is worth noting that description is not confined to words; much of 9/11 documentation was pictorial. Jean Baudrillard analyzed this mediation, concerned that “Even as the image exalts the event, it takes it hostage.”[11] He writes.

> This is what is always forgotten when we speak of the “danger” of the media. The image consumes the event by absorbing it and offering it up to the consumer. To be sure, it lends the event an unedited impact to a point, but it remains an image-event nonetheless… [b]ecause reality is a starting point, a first principle, and it's this principle that has been lost. Reality and fiction are inextricable, and fascination with the attack is above all fascination with the image.

The actual event of 9/11 was experienced in many ways, though, and the television images were only one. Patton, among many others, notes ”...the representation of events, in television and print media, has become part of the unfolding of events themselves."[12] He adds, “as Deleuze and Guattari point out, there is no reason why [their] conception of the pragmatics of language should be confined to spoken or written discourse…. [W]e can understand the media representation of a demonstration or a humanitarian crisis as integral to its actualization as a certain kind of event,” without reducing it to that representation.[13]

Sociologist Eric Fassin takes up a Deleuzian definition of events most significantly as a series of singularities. “[S]ingularities,” he argues, “only have meaning within the series that they delimit, dividing a past and a future: before the Affair, after the Affair. Both revealing and catalyzing, the Affair is thus nothing but the manifestation of a major social shift, a rupture in intelligibility.”[14] Fassin adds, "The event thus appears... as a break in intelligibility. But this is not simply an accidental feature of the landscape. The chasm of meaning does not open up by chance, in an aleatory way: there is nothing accidental about the event. The break in intelligibility, in fact, refers to a relation of power whose shift it makes apparent."[15] In his use of “appears” he marks that he seeks to identify breaks rather than create them.

Fassin and Alban Bensa try to pick up on certain series already in effect but hitherto invisible. The two proceed with an examination of possible series within which 9/11 might fit.[16] They suggest first the “grid” of international relations, and posit that 9/11 could be understood as the end of a strategic series of terrorist acts born of the Cold War, or a post-Cold War terrorism series. Shifting slightly, it could be, following Michel Feher, “the first post-colonial event.”[17] If colonialism involved battles fought on foreign soils in which the colonized were merely grist for the cannon, the attacks on New York and

[10] Patton, "The World Seen from Within: Deleuze and the Philosophy of Events."
[11] Jean Baudrillard, "L’esprit Du Terrorisme " *Harpers*, February 2002, 17.
[12] Patton, "The World Seen from Within: Deleuze and the Philosophy of Events."
[13] Ibid.
[14] Eric Fassin, "Sexual Events: From Clarence Thomas to Monica Lewinsky," *Differences: A Journal of Feminist Cultural Studies* 13, no. 2 (2002).
[15] Ibid.
[16] Alban Bensa and Eric Fassin, "Qu'est-Ce Qu'un Événement? Les Sciences Sociales Face À L’événement," *Terrain, revue d'ethnologie de l'Europe* 6 mars 2002.
[17] Ibid.

Washington were a version with reversed exoticism in the heart of the “west”; the deaths paralleled so many others in Cold War proxy battles.

Another grid is that of American history, for which they propose 9/11 not as the end, but the beginning of a series relating to valorization of the public domain. They align this possible domain more closely to class than race or gender, yet in a social rather then or at least in addition to, economic register. In the images of the 11th of September, aftermath and recovery, they identify a new kind of working-class hero, connected to the legitimacy in public service of the firemen, policemen and yet all the victims as well. They point to the remediation of the flag of the Reagan conservative years, which had been defined against the Vietnam generation's rejection, into a subtly different symbol. What they describe, they admit, may be short lived and perhaps only secondary. It is easier to correctly diagnose in hindsight, to identify when “sense” broke down, than to identify in real time the opening of a series and assess what it means.

Government reorganization came out of a certain understanding of what had occurred and why. The moment of the working-class hero they diagnose, even if already passed, was the one in which current policy was designed and put into action, and was also the moment when state and local law enforcement officers began to move into counterterrorism. The specific ways 9/11 was described and interpreted directed the changes that were implemented. This brings us back to how 9/11 was actualized, beginning with the role of Pearl Harbor and “intelligence failure” in defining the event, and the series in which those specific rhetorical resources themselves fit.

Pearl Harbor

President George W. Bush wrote to his diary on September 11, 2001, “The Pearl Harbor of the 21st century took place today.”[18] 9/11 was the deadliest and most expensive peacetime attack on US shores since 60 years earlier,[19] yet the analogy is not straightforward. Both sides are burdened with mixed meaning. Certainly Pearl Harbor was a point of reference on September 11th and in subsequent reporting and analysis. As historian Emily Rosenberg observed, "No one needed to command the widespread use of Pearl Harbor imagery. Commentators around the country spontaneously invoked it, and many Americans seemed actually to 'experience' the attacks through the memories that the Pear Harbor-hyped summer of 2001 had helped forged.”[20]

What “Pearl Harbor” itself means, however, has evolved over the years. Making sense of a World War II disaster, its ostensible causes and inferred messages, has been a contested process from the start. Government-sponsored committees, active stakeholders (such as the relatives or supporters of the men who took the blame) together with those interested in its possible lessons did long work of research and reacticulation. These were often construed during the Cold War as indicating intelligence and defense buildup. History, Rosenberg points out, is not an avenue “to ‘recover’ some ‘authentic’ version of the past but…[is rather] ever-changing and inevitably mediated fields of

[18] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 174.

[19] In fact, in August, 1998 Osama bin Laden's terrorist network "succeeded in carrying out two sophisticated, simultaneous, and devastating truck bomb attacks against the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, killing 224 people and injuring 5,000 more". inAmy Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security* 29, no. 4 (2005).

[20] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 174.

contestation over how to structure the past's representation."[21] Different groups vied to have their account and/or explanation accepted as official. The shifts and versions must be examined, then, in order to see what those connecting Pearl Harbor to 9/11 are referencing, or claiming and promoting.

At 7:50 AM PST on December 7, 1941, the Japanese air strike commander signaled the beginning of a raid that would damage or destroy most of the US Army and Navy war craft stationed in Hawaii, and leave 1,178 Americans wounded and 2,403 dead.[22] Although an attack had been long suspected, the date and location were not identified in a morass of intelligence information; surprise was complete and humiliating. The two countries had been and still were in diplomatic negotiations, adding to a US feeling of betrayal. The United States quickly declared war on Japan, followed with declarations against Germany and the other Axis powers. An investigation into who should take the blame, the first of ten (the last concluded in 1995), was launched within two weeks.

With this brief outline, some reasons for the Pearl Harbor–9/11 analogy are obvious (and some differences highlighted). Both were destructive attacks, and successfully caught the targets and general population by surprise. They were also literally attacks *on* the United States, or at least, Pearl Harbor was carefully presented, and remembered, that way: Roosevelt crafted his message to emphasize the "Hawaiian Islands," not yet a state, over the other Japanese attacks in the Pacific.[23] 2001 was also the crescendo of the World War II adulation begun in the 1970s. It was the 60th anniversary of the air strike, and an eponymous Hollywood mega production had been released at the beginning of summer, after an extravagant build-up that aimed to make attending the movie a patriotic act, a kind of vicarious participation in the (just and victorious) "Good War."[24] The film avoided potentially touchy subjects, such as American military inadequacy before the strike, denigration of Japanese character, possible negligence by responsible individuals or the isolationist refusal to enter World War II. In its ahistoricity and general mediocrity (aside from special effects), the result was a memorable title for a generic tale, the details forgettable.

Rosenberg convincingly argues that, in repackaging certain traditional narratives, the movie placed Pearl Harbor in the tradition of Custer's last stand and the Alamo. These were frontier myths where defeats became opportunities for virile revenge, transforming ignominy into triumph and placing an emblematic failure within a greater story of success.[25] The movie's familiarization of the name Pearl Harbor, without specific historical content, made it into a mnemonic for well-known story outlines onto which 9/11 could be grafted. Victim became hero became patriot; harm was suffered, followed by struggle, then triumph. Pearl Harbor from the perspective of history was subtly heartening—it had, after all, been avenged. Official presidential pronouncements after 9/11 employed the frontier / Old West leitmotif, with its implicit assertion of eventual victory. On September

[21] Ibid., 3.

[22] Gordon W. Prange, Doland M. Goldstein, and Katherine V. Dillon, *Pearl Harbor: The Verdict of History* (New York: McGraw-Hill 1986), xxxi-xxxii.

[23] Franklin D. Roosevelt, "7 December Proposed Message to the Congress," http://www.archives.gov/education/lessons/day-of-infamy.Other strikes included the Philippines, then a commonwealth, and Guam, an unincorporated territory.

[24] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 172. "Before the widespread publicity for Pearl Harbor, market research had shown that young adults aged 19-24 generally could not identify Pearl Harbor" cf Jess Cagle, "Cinema," Time, June 4, 2001, 69

[25] Ibid.

15th, George W. Bush swore, “we will find those who did it; we will smoke them out of their holes; we will get them running and we'll bring them to justice.”[26] Two days later, he added, “I want justice. There's an old poster out west, as I recall, that said, ‘Wanted: Dead or Alive.’”[27] The Pearl Harbor analogy also indicated a course of action. Lance Morrow, in *Time* magazine’s first issue after 9/11, held up a starting gate banner: “A day cannot live in infamy without the nourishment of rage. Let's have rage. What's needed is a unified, unifying, Pearl Harbor sort of purple American fury—a ruthless indignation that doesn't leak away in a week or two.”[28]

The administration further capitalized on the 9/11–Pearl Harbor association by extending the analogy to World War II and its “war on terrorism.” The connection asserted the war on terror as the next great civilizational struggle, a successor to WWII and the Cold War: “What happened at Pearl Harbor was the start of a long and terrible war for America,” Bush pronounced.[29] “Yet, out of that surprise attack grew a steadfast resolve that made America freedom's defender. And that mission—our great calling—continues to this hour, as the brave men and women of our military fight the forces of terror in Afghanistan and around the world.”[30] The war of retaliation against the Afghanistan Taliban for providing safe harbor to al-Qaeda was followed by the war to depose Iraqi president Saddam Hussein. The invasions were rhetorically linked as part of the broader symbolic battle for democracy and “fundamental human freedoms.”[31] Subsequent to both, Bush proclaimed, “we are again a nation at war. Once again, war came to our shores with a surprise attack that killed thousands in cold blood. Once again, we face determined enemies who follow a ruthless ideology that despises everything America stands for. Once again, America and our allies are waging a global campaign with forces deployed on virtually every continent. And once again, we will not rest until victory is America's and our freedom is secure.”[32] The heroic framing of the war on terrorism was successful for only a short time, but its ability to produce long lasting consequences were in part to the persuasive allure of the earlier period.[33]

[26] George W. Bush, "Transcript of Remarks by the President, Secretary of State Colin Powell and Attorney General John Ashcroft: President Urges Readiness and Patience, September 15th, 2001," Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2001/09/20010915-4.html

[27] ———, "Transcript of Remarks by the President to Employees at the Pentagon: Guard and Reserves "Define Spirit of America, September 17th, 2001," Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2001/09/20010917-3.html.

[28] Lance Morrow, "The Case for Rage and Retribution," *TIme Magazine*, 14 September 2001.

[29] George W. Bush, "Transcript of President's Remarks on the Uss Enterprise on Pearl Harbor Day: We're Fighting to Win - and Win We Will, 7 December, 2001," Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2001/12/20011207.html.

[30] Ibid.

[31] ———, "Transcript of President Commemorates 60th Anniversary of V-J Day, August 30th, 2005," Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2005/08/20050830-1.html

[32] Ibid.

[33] For a good review of the “cottage industry” that sprang up and the way this affected media, from publishing to television and cinema, see Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*.; David Hoogland Noon, "Operation Enduring Analogy: World War Ii, the War on Terror, and the Uses of Historical Memory," *Rhetoric & Public Affairs* 7, no. 3 (2004).; Christopher Hayes, "The Good War on Terror: How the Greatest Generation Helped Pave the Road to Baghdad," *In These Times*, no. 8 September (2006), http://www.inthesetimes.com/main/article/2788/.

"War" itself was perhaps a useful mobilizing tool. Historian David H. Noon summarizes the common argument that Americans define themselves through wars, literally or figuratively, writing: "Strictly speaking, the idea of a 'postwar' American culture is unintelligible."[34] He refers not just to American military engagements, but also to the way that social policy versions of wars (on drugs, or the trade war with Japan) appear in the absence of a major mobilizing political and military agenda such as Korea, or the Cold War against Communism. Combining domestic and international counterterrorism into a "war on terrorism" comes in this tradition. The definition of victory has in these social policy campaigns has often been vague, which might be interpreted as intentional, a way to allow their continuation despite the lack of signs of advancement. The "War on Drugs" did not keep drugs from entering the US, nor away from the population. It was effective instead as way to get resources to law enforcement, as justification for international policy both related and unrelated to drugs, and a way of maintaining budget, equipment and personnel skills in the absence of major conflict.[35]

While successful in these latter goals, withal, social policy campaigns do not mobilize government or society in the same way that a human enemy does. One retired narcotics agent, Jon, scoffed in an interview in early 2005 that the war on drugs was never a war: "[A]t most there was a heated skirmish. War when it is used that way is a political term. It's used when someone's kid dies, to say 'we're doing something.' It's a catchword, it says we're putting forth maximum effort, joining together against a threat, a common enemy, or the source of a threat." Jon described it essentially as a rhetorical strategy. Casting domestic counterterrorism as war can then be partly understood in this tradition of American politics. Hence the history of presenting social policy as war is also a cautionary tale, given its limited effectiveness.

Another reason to frame the "war on terror" through World War II is the prodigious prestige the latter has acquired, notable in an extensive "memory boom."[36] Messy actuality cannot compete with the rosy glow of memory and moral certainty yielded by the editing of time and nostalgia. A suitable distance in the past, that war seemed to fill a romantic void for which Vietnam and social policy programs were unfit. Studs Terkel's Pulitzer Prize winning "The Good War" (1984), Tom Brokaw's television series "The Greatest Generation," a long series of Stephan Ambrose books (including "*Citizen Soldiers*, *Band of Brothers*, *The Wild Blue*, and *D-Day*, as well as five edited volumes, contributions to six essay collections, forwards to 18 books written by others, and a 2001 calendar"), among innumerable other examples, gave proof to a huge market for World War II before September 11, 2001.[37] Museums and memorials were dedicated, and movies such as *Saving Private Ryan* (1998) were produced. The Arts and Entertainment Network identified such a strong trend that they established the History Channel, "an

[34] Noon, "Operation Enduring Analogy: World War Ii, the War on Terror, and the Uses of Historical Memory."

[35] Steven R. Belenko, ed. *Drugs and Drug Policy in America: A Documentary History* (Westport, CT: Greenwood Press,2000), 307.The 1986 Anti- drug Abuse Act, in which drugs were declared a national security problem and a threat to the international community, "called for enhanced interdiction efforts by the Defense Department and provided $278 million to purchase or refurbish eight airplanes, eight helicopters, and seven radar aerostats. In all, the 1986 act authorized $1.7 billion in new money to fight drug abuse. Only $231 million (about 14 percent) was allocated for treatment, education, and prevention efforts".

[36] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 113-25.

[37] Noon, "Operation Enduring Analogy: World War Ii, the War on Terror, and the Uses of Historical Memory."

instant hit."[38] Trenchantly, "Documentaries about the World War II era proved so popular and pervasive that some channel surfers satirically dubbed it the "Hitler-Channel."[39]

Rough edges were smoothed over in the transformation of World War II into resonant American mythology. Before this happened, Pearl Harbor was for years discussed as a failure of the American people. The Lynchburg News's early self-chastisement ("our blindness, our provincialism, our complacency, even our ignorance as a people") was later echoed by President Truman's pronouncement that "the country as a whole is basically responsible in that the people were unwilling to take adequate measures to defense [sic] until it was too late to repair the consequences of their failure to do so."[40] As late as 1979, Vice President Walter Mondale remarked that the United States and other nations "failed the test of civilization" by not doing more, sooner, for European refugees."[41] After Pearl Harbor, industrial, government and civilian resources began to be mobilized, but as historian Gordon W. Prange admonished, "one must not exaggerate the type of unity the Japanese bestowed upon the Americans. The entire nation had not suddenly become of a unanimous mind," but rather "the national energies had mobilized to achieve a single, readily identifiable goal."[42] In the words of one Roosevelt opponent, "It is the feeling of the man in the street that he tricked us into this war."[43] Roosevelt had campaigned on the promise of not entering a "foreign war," underplaying that a domestic strike would of course make it an American war. Decrying such verbal subtlety as chicanery, his detractors developed the "backdoor theory," that "the president and his advisors had schemed to provoke Japan, deliberately withheld any warning, and orchestrated a massive coverup."[44] A long series of investigations stemmed partially from this theory, partially from the fact that blame was assigned to the responsible military commanders, whom many claimed were scapegoated. These results were to have a direct impact on the 9/11 Commission.[45]

The notable point here is that entrance into World War II and the war itself were still subject to critique. Since that time, World War II has been imbued with unassailable morality. The enormity of Holocaust lent support to a simplified national self-narrative, in which the United States was goaded into action by Pearl Harbor, but in fact entered the war to save the Jews. As Noon points out, however, "the centrality of the Holocaust in American popular memory of World War II was belated, linked more to the events of the 1960s, bracketed by the trial of Adolph Eichmann in 1961 and the Six-Day War in 1967.[46] US actions were enfolded in another American narrative, "of a nation that summons its economic and military strength to create a better world," or in the words of President G.W.

[38] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 121.
[39] Ibid.
[40] Lynchburg *News*, December 10th, 1941 *in* Prange, Goldstein, and Dillon, *Pearl Harbor: The Verdict of History*.
[41] Noon, "Operation Enduring Analogy: World War Ii, the War on Terror, and the Uses of Historical Memory."
[42] Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York: McGraw-Hill, 1981), 737-38.
[43] Prange, Goldstein, and Dillon, *Pearl Harbor: The Verdict of History*, 92.
[44] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 42.
[45] James J. Wirtz, "Responding to Surprise," *Annual Review of Political Science* 9, no. 6 April (2006).
[46] Noon, "Operation Enduring Analogy: World War Ii, the War on Terror, and the Uses of Historical Memory." See Noon, footnotes 26-27 for a review of the literature critiquing Holocaust memory and U.S. policy

Bush, prefers “greatness to power and justice to glory.”[47] World War II would not have been so appealing as a motivational metaphor for the war on terrorism if it had not, as Christopher Hayes argues, been “scrubbed clean of its moral complexity. There is no mention of American big business financing the build-up of the Nazi war machine, no America First campaign determined not to shed American blood for European Jews, no firebombing of civilians in Dresden.”[48]

In addition to providing a symbolic lineage, viewing 9/11 through the prism of Pearl Harbor and World War II had other, heuristic effects. The emotive connection with history was politically advantageous, aiding to push through a Bush-administration agenda, but, clearly, that history also influenced perceptions about what needed to change and how. Much governmental and scholarly understanding of what constitutes intelligence failure and its causes has been developed through analysis of World War II. James Wirtz, in a review article comparing responses to both attacks, noted, "The Pearl Harbor experience, especially the history of the investigations that followed and Wohlstetter’s (1962) seminal study *Pearl Harbor: Warning and Decision*, exerted an important influence on the way scholars and officials approached the post mortem of the September 11 tragedy."[49]

Intelligence Failure

The 9/11 Commission, a primary player in actualizing manifold singularities into a recognizable event, tried to avoid the accusations of scapegoating and partisanship that had hounded the Pearl Harbor investigation by producing a unanimous report. At the same time, they purposefully set out to do what Roberta Wohlstetter had recommended in her study on surprise and intelligence, which was to produce documentation of the historical context within which decisions were made and facts interpreted. Wohlstetter’s main points, echoed by many others, were drawn from reams of Pearl Harbor archives. They can also be found everywhere from public pronouncements by the Executive cabinet to the Commission’s report. This view of intelligence, its possibilities and limits, was what resulted in changes in law enforcement and criminal intelligence.

The verdict pronounced on September 11th was repeated in newspapers the following day: “the failure to penetrate the plot in advance constitutes ‘an intelligence failure,’” said the vice chairman of the Senate intelligence committee, Alabama Senator Richard C. Shelby.[50] Those hesitant to jump the gun seemed nonetheless in counterpoint to this dominant narrative. The chairman of the intelligence committee, Florida democratic Senator Bob Graham, “told reporters that it was ‘premature’ to label the lack of warning as an intelligence failure. But Mr. Graham conceded that there were "ongoing weaknesses that we need to address in the intelligence community.”[51] By October 7, it was stated that “In hindsight, it is becoming clear that the CIA, FBI and other agencies had significant

[47] Ibid. In Noon, George W. Bush, "Transcript of Governor George W. Bush's Remarks: A Distinctly American Internationalism, December 19th, 1999," FAS, http://www.fas.org/news/usa/1999/11/991119-bush-foreignpolicy.htm.

[48] Hayes, "The Good War on Terror: How the Greatest Generation Helped Pave the Road to Baghdad."

[49] Wirtz, "Responding to Surprise."

[50] James Risen and David Johnston, "Officials Say They Saw No Signs of Increased Terrorist Activity," *New York Times*, 12 September 2001.

[51] Ibid.

fragments of information that, under ideal circumstances, could have provided some warning if they had all been pieced together and shared rapidly."[52]

The intelligence failure label stuck, and on one level, the "failure" is straightforward: planes were successfully hijacked, crashed into buildings, and no one seemed to have known this would happen. What else could this be, but a failure, and if the intelligence community were the ones supposed to have information, surely they failed. Yet as the history of Pearl Harbor and its ten investigations in order to assign blame have indicated, such a conclusion is anything but uncomplicated. To begin, it is necessary to specify what those people asserting intelligence failure mean and how the causes of failure are understood.

Anthropologist Rob Johnston studied analytical methods in the US intelligence community (comprised of sixteen members, each with multiple agencies, services, bureaus, and other organizations). From "489 interviews, direct observations, participant observations, and focus groups..." as well as "personal letters, email exchanges, and archival material," he developed composite definitions for intelligence, analysis and intelligence failure.[53] Johnston reported that for his informants, "Intelligence errors are factual inaccuracies in analysis resulting from poor or missing data; intelligence failure is systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses."[54] One can make a decision between two options and be wrong. But if something entirely different happens and one is surprised, then intelligence has failed. The literature on intelligence failure is, in point of fact, that of "strategic surprise." Parker and Stern's review of this literature found that (paraphrasing) "strategic surprise" is the abrupt revelation that one has been working with a faulty threat perception regarding an acute, imminent danger posed by a foreign threat to core national values, which often occurs after being victimized by an attack or a sudden shift in the security environment.[55] Breaking this down, "first, the attack is contrary to the victim's expectations; second, there is a failure of advanced warning; and third, the attack lays bare the lack of adequate preparation."[56]

Roberta Wohlstetter's 1962 book *Pearl Harbor: Warning and Decision* sifted through what information had been available before that attack, the way it was organized, and the bureaucratic structure, in order to figure out how and why the United States had been surprised by the Japanese raid. "If our intelligence system and all our other channels of information failed to produce an accurate image of Japanese intentions and capabilities," she observed, "it was not for want of relevant materials. Never before have we had so complete an intelligence picture of the enemy." (The same has been noted in even stronger language about 9/11.)[57] Rather than a lack of information, the problem is

[52] James Risen, "In Hindsight, C.I.A. Sees Flaws That Hindered Efforts on Terror," *New York Times*, 7 October 2001.

[53] Rob Johnston, *Analytic Culture in the Us Intelligence Community: An Ethnographic Study* (Washington DC: Central Intelligence Agency, 2005), xx. It is not necessary to get into a full discussion of intelligence or its process here (Chapter 4), as they are conceptually fairly distinct.

[54] Ibid., 6.

[55] Charles F. Parker and Eric K. Stern, "Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise " *Foreign Policy Analysis* 1(2005).

[56] E. Kam, *Surprise Attack: The Victim's Perspective* (Cambridge: Harvard University Press. , 1988), 213. *In* Parker and Stern, "Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise ".

[57] Roberta Wohlstetter, "Signals and Noise: The Intelligence Picture," in *Pearl Harbor: Roosevelt and the Coming of the War*, ed. George Macgregor Waller, *Problems in American Civilization*

that it is "much easier *after* the event to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear; we can see now what disaster it was signaling, since the disaster has occurred. But before the event it is obscure and pregnant with conflicting meanings."[58] Some percentage of failure, she concluded, is inherent to the practice of intelligence.

Wohlstetter wrote that she was "concerned almost exclusively with the facts of warning and surprise and their implications for today." To wit, her focus was what could be gleaned about the practice of intelligence, and indirectly, the proper implications for policy. Rosenberg, in her timeline of what Pearl Harbor has variously meant, writes that when Wohlstetter's book was published, "Implicitly, her thesis backed post-Bay of Pigs proposals for a more active, better funded intelligence agency, an agenda that her husband, security analyst Albert Wohlstetter, advocated over the next decade as he warned against underestimating the Soviet threat."[59] At least as significant as support for an already-common Cold War view, however, was the inference that if failure is evitable, one must aim for preparedness. Wirtz notes,

> The idea that a secure-second strike force must ride out a nuclear attack and survive, an extraordinarily expensive and problematic standard of effectiveness, became a centerpiece of US nuclear deterrent strategy. Wohlstetter's message…suggested to policy makers that it was easier and more prudent to protect weapons systems from a nuclear-armed adversary than to count on policy makers, analysts, and military commanders to respond effectively to signals of impending attack.[60]

The recommendations on intelligence and preparedness stemming from the Pearl Harbor investigations and subsequent review have been repeated nearly verbatim in analyses of 9/11: reorganize intelligence, create a central authority and so forth. Yet by dint of verbal contortions, the authors of the 9/11 Commission Report did not label 9/11 an intelligence failure; the phrase did not appear in their 585 page document. Instead, after quoting Wohlstetter on the inherent difficulty of sorting data, they wrote, "we asked ourselves, before we judged others, whether the insights that seem apparent now would really have been meaningful at the time, given the limits of what people then could reasonably have known or done. We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management."[61] Even if the 9/11 Truth Movement conspiracy theorists are correct and no one in power was actually surprised because they had orchestrated a media event to push a war agenda, the Commission's missing "failure" bears further consideration.

Mindful of the troubled Pearl Harbor investigations, the Commission hoped to produce a document that was analytically precise and judgmentally vague. The investigation avoided localizing blame not only in individuals, but also in the system, as that could lead to blame on those who had not changed the system in the Clinton or Bush administrations. The generous reading of this decision on the Commission's part is that

(Boston: Heath, 1965), 83.

[58] ———, *Pearl Harbor: Warning and Decision* (Stanford: Sanford University Press, 1962), 387. Cited in 9/11 Commission Report, 339

[59] Rosenberg, *A Date Which Will Live: Pearl Harbor in American Memory*, 44.

[60] Wirtz, "Responding to Surprise."

[61] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (New York: W.W. Norton, 2004), 339.

blame would lead to accusations of partisanship, and impede efforts at improvement. By "not identifying individuals whose acts of omission or commission directly contributed to the success of the al Qaeda attacks, and…not creating a list of failures that could be used as the basis of a political indictment of any government organization or administration," the country could focus on fixing the problems themselves.[62] In order to walk this thin line, and refrain from assigning accountability, the 9/11 Commission took up academic discussions such as Wohlstetter's about the inherent limitations of intelligence.

Critics did not have a generous reading, and the evaluation of the Commission's position as rational or only expedient depends on if the danger of al Qaeda was clear enough that inaction was negligence. If so, specific people could be held accountable. For Pearl Harbor, two people were found officially negligent and removed from duty, and General George C. Marshall, then Army Chief of Staff and a celebrated hero, was severely criticized. In relation to individual responsibility, Wirtz, among many others, makes the case that intelligence analysts and "policy makers prior to September 11 were even better informed about their potential opponent's intentions than their counterparts in the Roosevelt administration."[63] One critique of the Commission's report notes "Tellingly, the historical and analytical sections of the commission's report do not indicate or argue that the US government was improperly organized prior to 9/11."[64] Arguing structural problems and individual negligence, Richard Clarke, the National Coordinator for Counterterrorism when the attacks occurred, writes:

> Somewhere in the CIA there was information that two known al Qaeda terrorists had come into the United States. Somewhere in FBI there was information that strange things had been going on at flight schools in the United States...red lights and bells should have been going off. They had specific information about individual terrorists from which one could have deduced what was about to happen.[65]

Successful "surprise" attacks are understood to be avoidable and yet inevitable. Any given failure could have been avoided if the right actions were taken, but it is impossible to always take the right actions. Ephraim Kam, a political scientist and analyst in the Israeli Department of Defense, surmises along the lines of Wohlstetter that "it is doubtful whether one can ever really determine who is to be blamed for estimate failure. On the one hand analysts and decision makers are interdependent and share responsibility for failure; on the other, since surprise attack is common, indeed almost inevitable, it is questionable whether anybody should be blamed for the failure to prevent it."[66] The litany of missed opportunities to stop the attacks on the World Trade Center and the Pentagon grew quickly after the attacks: hijackers known by the CIA to be terrorists were given US visas by an unsuspecting State Department; a report had come from Arizona that middle easterners with radical ideology were learning how to fly; ten out of nineteen hijackers

[62] ———, "Responding to Surprise."
[63] Ibid.
[64] Richard A. Falkenrath, "The 9/11 Commission Report : A Review Essay " *International Security* 29 no. 3 Winter 2004/05 (2005).
[65] Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004), 236-37.
[66] Ephraim Kam, *Surprise Attack : The Victim's Perspective* (Cambridge: Harvard University Press, 2004), 215.

were identified but no one thought to not let them on the plane—procedure was only to hold their bags until they had boarded. The list goes on.

While in retrospect these omissions or malfunctions stand out, at the time, the argument goes, correct prioritization was not possible. Kam discusses the difficulty in eliminating errors in intelligence estimates, but he reminds that the "failure to prevent a surprise attack does not evolve overnight'" nor is it "the result of any single factor…[or] mistakes committed on any one level."[67] A singular incident and organizational failure have different temporalities, a point which is intuitively grasped. It is therefore not so easy to blame the actors who did not change the structure and laws guiding the intelligence community. There was, however, a way to put the system on alert. The key actors are held accountable by positing that if they had given ample generalized warning that something dire was going to occur, and put the whole system on alert in the manner of the millennium threat, 9/11 could have been averted. This moves the failure, or cause of surprise, from faulty intelligence operations and organization to the implementation of policy. The counterpoint is that the people in charge must weigh "known" versus only potential costs. "Commanders," Wirtz observes, are "hampered by a sensitivity to the known costs of maintaining a heightened state of readiness, such as loss of training time and wear and tear on equipment and personnel, compared to the potential costs of enemy action."[68] He adds, "no method has been devised to overcome the basic problem Wohlstetter identified more than 40 years ago: Warnings will always appear to be ambiguous, if not dubious, while the costs of responding to the possibility of enemy action will be clear and high."[69]

The 9/11 Commission, resolute, refused to evaluate if someone should have taken general actions to step up security in the face of clear warnings that *something* was going to happen. On the absence of preventative security measures, Richard Falkenrath contended that this constituted "failures of performance by specific government officials, whom the commission elected not to criticize directly."[70] Political scientist Amy Zegart countered by arguing that too much attention has been paid to individual failure, and it is instead necessary to change pathologies in either structure and organization, or "culture." The efforts of Zegart to shift the focus away from individual blame could be seen as biased in that she studied under Condoleezza Rice, the US National Security Advisor from 2001–2005. (Zegart's work, however, had always been on the bureaucracy of national security agencies.) For those who felt that government procedures had not kept pace with the world, the silver lining in the destruction of potent American symbols was the space for change that was opened. "America," lamented Richard Clarke, "seems only to respond well to disasters, to be undistracted by warnings."[71] Immune to suggestions of her own culpability, National Security Advisor Rice found it "tragic" that it sometimes happens that "until there is a catastrophic event that forces people to think differently, that forces people to overcome all customs and old culture and old fears about domestic intelligence and the relationship, that you don't get that kind of change."[72]

[67] Ibid., 213.
[68] Wirtz, "Responding to Surprise."
[69] Ibid.
[70] Falkenrath, "The 9/11 Commission Report : A Review Essay ".
[71] Clarke, *Against All Enemies: Inside America's War on Terror*, 238.
[72] Condoleezza Rice, "Transcript of Dr. Conoleezza Rice's 9/11 Commission Statement Wednesday, May 19, 2004," CNN, http://www.cnn.com/2004/ALLPOLITICS/04/08/rice.transcript/.

The “old fears about domestic intelligence” were of course rooted in a long history of law enforcement abuses, but the Bush administration capitalized on the moment to push through both structural and legislative changes. Two significant approaches prevailed: preparedness and prevention, especially through preemption. The latter idea, advanced through the PATRIOT Act, would have its far-reaching implications for law enforcement. Turning the metaphor of global war into domestic practices proved contentious, in fact, as did the role of the Pentagon in enacting those changes. Zegart placed much of the blame for bureaucracies failure to adapt to a changing world and the need for a new approach, even after the attacks, at the Department of Defense: “There's a reason why no president since Harry S. Truman has gotten serious about overhauling intelligence agencies through executive orders or legislation. It's called the Pentagon. For decades, the Defense Department has controlled about 80 percent of the intelligence budget and housed most of the agencies. And for decades, it has fiercely resisted any move to realign power in the CIA or anywhere else.”[73]

The “war on terrorism,” Jon, the former narcotics agent commented, "is against people. It’s a war model. We always prosecuted the war on drugs as criminal justice, locking people up and taking them to jail, not killing them. It was a criminal model.” The criminal justice model does not tend to produce the kind of black and white case that lends itself to patriotic fervor or later, nostalgic devotion. This boded poorly for its status as a generational crusade. “Whatever the natural similarities between December 7, 1941, and September 11, 2001,” Christopher Hayes remarked in connecting the World War II adulation with the War in Iraq, “the association of the two has led us to convert—first in rhetoric, later in fact—a battle against a small band of clever, murderous fundamentalists into a worldwide war of epic scale.”[74] The rhetoric gradually began to shift, even during the Bush administration, and police as well. This led to alternatives such “global counterinsurgency” abroad, and more subtly, a focus on security, rather than danger, at home.[75] The legislation that had been passed, however, remained in place, including government powers related to surveillance, searches and habeas corpus, precisely at the elided war–crime nexus to which Jon pointed.

After the September 11th attacks, Zegart began studying the intelligence community’s previous design and subsequent reorganization. She combed through twelve government-commissioned reviews of the intelligence system between the fall of the Soviet Union and the fall of 2001, and concluded that there was “surprising agreement on four major problems.”[76] The intelligence community lacked a sense of community, the personnel systems did not encourage personnel to develop the right skills or to share information with each other, the system for setting intelligence priorities was weak and—most germane to this dissertation—there was simply insufficient human intelligence.

Terrorism as crime?

The FBI, by mandate, was responsible for domestic terrorism. The problem was the infamous “wall” between its investigative functions that ended in the criminal justice system, and an ideally preventative intelligence process. Six years into the reorganization

[73] Amy Zegart, "Our Clueless Intelligence System," *Washington Post*, 8 July 2007.

[74] Hayes, "The Good War on Terror: How the Greatest Generation Helped Pave the Road to Baghdad."

[75] Rieff, "Policing Terrorism."; David Kilcullen, "Ethics, Politics, and Non-State Warfare: A Response to GonzáLez," *Anthropology Today* 23, no. 3 (2007).

[76] Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies."

of the intelligence community, “The ‘new FBI’ is still fighting the old FBI's cops-and-robbers culture,” Zegart admonished, with descriptive examples:

> Visit the bureau's Web site, where job postings are divided into two categories—special agents who wear badges, carry guns and catch bad guys, and everyone else. Analysts, those dot-connectors who since 9/11 have been touted as equal partners in the FBI's counterterrorism mission, are still relegated to "professional support staff," alongside auto mechanics and janitors.[77]

Privileging criminal cases had another effect. The reputation of FBI agents as “men of action,” was partly the legacy of J. Edgar Hoover’s public relations machine. He “worked assiduously to develop a culture and image of FBI agents... In 1935 alone, 65 movies featured the FBI. All of them glorified FBI agents as intrepid heroes, guns in hand, who worked the streets to solve crimes and always got their man."[78] The problem, as one FBI agent put it me, was “we don’t know anyone. Local cops, they know everyone.”

[77] ———, "Our Clueless Intelligence System."

[78] Amy Zegart, "9/11 and the Fbi: The Organizational Roots of Failure " *Intelligence & National Security* 22, no. 2 (2007).

Chapter Six. Collecting the Dots

"Every terrorism case that I've ever worked has been started by a patrolman," Jerome, the deputy director of the fusion center told me. We were in his office, the door shut to keep out the sound of the flat screen TV tuned to FOX news. "It has always been a patrolman," he went on. "It is not going to be your FBI agent, your CIA officer reporting these things to you and saying, 'here is the bad guy.'" Jerome's comment summed up the logic of integrating state and local law enforcement into homeland security. His belief, based on personal experience, attains the status of general truth as it ascends government circles. "We all know that it won't be a bureaucrat in Washington who will thwart the next terrorist attack,"[1] was how Representative Jane Harmon (D-CA) put it at a House Subcommittee hearing.

> [A] diligent police or sheriffs' officer somewhere in America—during the course of his or her daily work—will see something or someone out of place, and guided by timely, accurate and actionable information, will connect the dots that will unravel a plot in-the-making.[2]

"We have to *collect* and *connect* the dots," added California's Executive Director of Homeland Security. The job, he extrapolated, belonged to cops and analysts.[3]

The government-wide plan for "collecting and connecting the dots" is called the National Information Sharing Environment Suspicious Activity Reporting Initiative (ISE-SAR).[4] Suspicious Activity Reports are inputs of information to a larger, comprehensive project to coordinate "policies, rules, standards, architectures, and systems." The goal is to produce a unified information system, rather than one divided along the lines of government bureaucracies. The concept of operations is that cops describe suspicious activities, potentially terrorist-related, in reports. These are sent to analysts at regionally run fusion centers, nodes in the national system. Analysts put pieces together and search for links. Data are vetted, standardized and, if deemed relevant to a terrorism nexus, distributed in the environment. Follow-up is generally done by the FBI, which holds responsibility for domestic terrorism, perhaps in conjunction with the reporting entity. The picture drawn of real-world organizations and their plots are supposed to be relayed back down the line in a form which state and local law enforcement can use to prioritize their own resources and counter threats. In the words of the Director of Homeland Security

[1] Jane Harmon, "Statement to the House, Subcommittee on Intelligence, Information Sharing & Terrorism Risk "The Future of Fusion Centers: Potential Promise and Dangers"," House of Representatives (Washington, DC: Committee on Homeland Security 2009).

[2] ———, "Statement to the House, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs"," (Washington, DC: Committee on Homeland Security 2008).

[3] Emphasis added. Matthew Bettenhausen, "Statement for 'Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs', Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment," House of Representatives (Washington, DC: Committee on Homeland Security 2008).

[4] "Nationwide Suspicious Activities Reporting Initiative: Fact Sheet," ed. Program Manager for the Information Sharing Environment (PM-ISE) (Office of the Director of National Intelligence, 2008).

Janet Napolitano in 2009, a “seamless network of information-sharing” will create a “seamless web of security.”[5] Knowledge will keep us safe.

Safe, though, from what? Although the Information Sharing Environment program emphasizes that it is not “building a massive new information system,”[6] rather leveraging what already exists, it is nonetheless an investment. Creating a seamless web to “detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America” might be seen as a profligate response to attacks that succeeded in killing three thousand people,[7] but not three hundred thousand, or three million. Inadequate health, education, standard of living and opportunity cause more harm to a greater numbers of people. In a world of limited means, the allocation of resources amounts to an ethical decision. More pointedly, the system itself has been decried as a threat. When legal barriers to domestic surveillance have been lowered to address security concerns, historically the result has been a coincident breach of civil liberties. Even before counterterrorism duties and authority are added to the mix between local police and the public, relations are often tense. What justifies such a system, when the odds are greater that one will be killed by a car, or a police officer, than a terrorist?

Mortality, however, was not the metric of September 11th. No one thought that the United States population level was threatened. Routine violence, from accidents to fatal disputes, inevitably kills many people, but its toll is proportional to the number of acts. Such violence too is viscidly familiar. Even the almost cyclical occurrences of police transgression, now often captured on video, are part of the quotidian rather than the exceptional. The danger of the attacks was understood as existential, but existential to a multiform set of values, a “way of life,” a political system. In the specter of terrorism with nuclear weapons or contagious, fatal disease, social and mortal fears are melded. Mass casualty terrorism may be “unlikely,” but probability is not a useful calculation if the rare event is regarded as too horrific to let happen. The creation of an “information sharing environment” was an approach that developed when a probabilistic calculus of risk, and a deterministic relationship between the present and the future, became understood as inadequate to dangers with asymmetrical consequences.[8]

The metaphor of dots codifies an otherwise infinite and messy realm of objects, people, interactions and behaviors. Units of action, objects, or behaviors can be documented, categorized, transferred, and assessed. They are pieces of the present, and future, which once discerned as such are available for intervention. It is a deft conceptualization of reality for the digital age. Yet vexingly, we are “drowning in data, but

[5] Janet Napolitano, "Remarks to the National Fusion Center Conference," (Kansas City, MO: Department of Homeland Security, 2009).
[6] "Information Sharing Environment Implementation Plan," Office of the Director of National Intelligence, http://www.ise.gov/pages/vision.html.
[7] Ibid.
[8] These tend to coexist, not supplant, other approaches to the future. In particular, see Fearnley, Lakoff and Collier. Fearnley on the use of the Monte Carlo technique in syndromic surveillance (unpub. manuscript). Lakoff on scenario-based exercises as a technique “to generate an affect of urgency in the absence of the event itself; and second, to generate knowledge about vulnerabilities in response capability that could then guide intervention” .Lakoff, "The Generic Threat, or How We Became Unprepared." Collier on “estimating the likelihood and consequence of potentially catastrophic future events”, not through archiving and statistical calculation of risk but through inventories and “enactment”. Stephen J. Collier, "Enacting Catastrophe: Preparedness, Insurance, Budgetary Rationalization," Economy and Society 37, no. 2 (2008).

starving for knowledge," constantly trying to clamber out of "data tombs."[9] The continuous accumulation of more data does not provide a solution. The reason is because knowledge is not the opposite of ignorance, but complementary to it. As the amount there is to know increases, the amount one doesn't know grows in tandem. As information accumulates, so do possibilities, and therefore uncertainty about the future and what to do. Yet the world has not, in fact, ground to a halt. Clearly, other ways of making decisions have been employed.

The goal of the Information Sharing Environment is not to prevent or prepare for an already-actualized event, such as another airplane attack. Ideally the ISE seeks to avoid "legacy futures," old conceptions of the future that constrain planning to imaginable events.[10] "Terrorists don't do movie plots," as one security expert put it.[11] Concretely, or at the real-world level of actions that become dots of data, the ISE cannot and does not quite aim to escape them, as we will see. Yet it does not constrict or limit the ever-growing mountains of data either. Instead, the ISE is designed to function as an agile assemblage that makes accessible the potential of data to discern a threat, even if its shape is unknown.[12] If information is composed of infinite dots, and within these are contained the potential of the future, the problem becomes how to pick out the significant ones. "What is significant" refers to sites where intervention is possible, across a wide range of registers. Strategy and operations present different temporalities and modes of action, as do local police department and national security agencies. There are also differences, unsurprisingly, between theory and practice.

This chapter is about the role of the police in the Information Sharing Environment. That is to say, it is about the use of law enforcement in intelligence gathering, and the inherent friction caused by a group with one set of rules and objectives being given a task that is governed by a different set of rules and objectives. The first step is the collection of information. "Suspicious activity" may be called in by someone, or observed in the course of duty. Cops, who are assumed to have experiential expertise in suspicious behaviors related to crime, are expected to learn those pertaining to terrorism. What constitutes an indicator of terrorism, and how a cop is supposed to recognize it, are two problems the ISE has aimed to resolve.

***

In Jerome's office, he continued his explanation of state and local law enforcement's role in counterterrorism:

> It is always a local cop who saw something. On face value, a guy with a bunch of stolen credit cards may be an insignificant thing. The officers book him for that, forget it, walk away, let him do his probation. They don't realize that while he's out on probation, he's raising money for a terrorist group. A lot of the officers have a misconception about what terrorism-related crimes are, because there is such a broad range of items it can be, other than just the guy out there doing the scouting, or the guy purchasing chemicals to make the bomb.

[9] "Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Assessment ", 186.

[10] Jamais Cascio, "Legacy Futures," *Open the Future*, 8 December 2008.

[11] Bruce Schneier, "Terrorists Don't Do Movie Plots," *Wired*, 8 September 2005.

[12] Paul Rabinow and Gaymon Bennett, *Synthetic Anthropos: Designs for Human Practice* (Connexions, 2008).

> Terrorism involves an enormous network of people. Basically a whole network is supplying one person, who may do a terrorist mission. To be able to do that, there is an incredible amount of work that needs to be done. There are people supplying them with money, supplying them with locations to live, basic food, clothing. It is a large network to take care of everything from the logistics of the people going out there and actually finding a good target, to locating that, to setting up the preparations in order to get the folks trained overseas.

Four ways that state and local cops are deputized in domestic counterterrorism are enfolded in Jerome's description, and will be laid out in order. First, law enforcement can directly track the movement of funds. Financial investigations, by focusing on the money, offer a pathway that law enforcement can follow back to different kinds of crimes. Some of the ways that funds are raised, such as charitable donations, would be perfectly legitimate except for their end use. Criminality therefore depends on whether the recipient is a "designated terrorist organization." This technicality has practical consequences. Second, cops are supposed to remain alert to signs of a possible connection to terrorism in the crimes they investigate. A "guy with a bunch of stolen credit cards" is committing an ordinary crime.[13] What is clear in this case is that the act is criminal in and of itself. If stolen credit cards are used to raise "money for a terrorist group," then he has committed the additional crime of terrorism financing.[14] Third, in the course of answering service calls or otherwise maintaining the peace, cops should similarly look for indications of terrorism.

The fourth and trickiest category is documenting "people going out there and actually finding a good target." "All around the world," protested one blogger, "cops and rent-a-cops are vigorously enforcing nonexistent anti-terrorist bans on photography in public places."[15] Public outcry and the poor results of "racial" profiling have led to the perhaps equally contentious, and difficult to separate solution of behavioral surveillance. Ostensibly ordinary behaviors present the same kind of shift in the locus of illegality as charitable fundraising: it is not the means but the end that count as crime. Separated from criminality, however, the indicators are largely activities protected by the First Amendment. There is no parallel to the "terrorist organization" designation, so the cop must conjecture suspect motive and intent.

Money Trails

Terrorist plots get the most attention, Jerome told me, but fundraising crimes and laundering the proceeds are more constant and widespread problems. Under federal law, money laundering is "the flow of cash or other valuables derived from, or intended to facilitate, the commission of a criminal offense. It is the movement of the fruits and instruments of crime."[16]

[13] An "ordinary crime" is that which is not subject to the laws that would make it a military or war crime. Here I narrow that category to mean an act such as theft or assault that is not committed for political, ideological, religious or personal purposes that might make it fall into the category of hate crime or terrorism. I avoid the term "common crime", since this can mean simply a lesser infraction, used in contrast with "felony."

[14] Matthew Levitt and Michael Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances," in *Policy Focus* (Washington Institute for Near East Policy, 2008).

[15] Cory Doctorow, "Fake Dhs "Photography License" For Fake No-Photos Laws," *Boing Boing*, 15 May 2009.

[16] Charles Doyle, "The USA Patriot Act: A Sketch," (Congressional Research Service, 2002).

“Millions of dollars here in the United States, and especially from here in California, are going overseas to support terrorism activities,” Jerome went on.

> Right now we’re like a bucket with a bunch of holes in it, and money is just flowing from this country, from this state. Often times people who are experts in terrorism will say the reason they feel that California hasn’t been hit by a major terrorist attack is because it would disrupt the flow of money to the Middle East—or to the Philippines or to Sri Lanka or to Afghanistan or to Iraq. So, I hate to believe it, but it kind of makes sense.

He touches on what has been called the "don’t-bite-the-hand-that-feeds-you” theory," that terrorist groups in the US are “unlikely to mount attacks within that country’s borders for fear of losing lucrative funding streams.”[17] On the other hand, the "presence-equals-threat theory" holds that "the groups fundraising or providing support functions within the country present a viable and immediate threat to the United States as those support networks could easily go operational."[18] Both ways, financial misdeeds can provide entry to a fuller terrorism investigation, as they have for other crimes for decades. “Looking at money laundering is a counternarcotics tactic,” a DEA agent told me, “and now drugs and terrorism are being fought the same way.” A retired IRS criminal investigator explained how, at least for domestic counterterrorism, this had taken place over the course of his career.

> All asset forfeiture prior to ‘83 was done by the IRS. To address proliferation of drug activity, we took away assets. No laws allowed for that except for tax purposes. US Title 26 granted the IRS this right, but no one else. So back then, the IRS had agents working DEA cases, FBI cases. A number of my friendships were developed in those days. Then came along Title 18 and 21, criminal procedure section 881 and 981. These granted DEA and FBI the right to seize assets. States followed suite, and passed legislation so that their police could seize assets.

The changes in assets forfeiture he described had many repercussions, dispersing the tactic of financial investigation and incentivizing its use for pet expenditures such as cutting-edge equipment. The relationships formed as a result of collaboration on cases remained important: a truism but one especially pertinent in law enforcement. The crime arena is legally compartmentalized into missions and permissible investigative tools. This is one of the reasons for physical co-location in taskforces and fusion centers. Creating interagency personal relationships is another: cooperation and exchange work on the basis of trust.

I asked IRS investigator, “Did terrorism come up, back in the 80s and 90s?” He responded.

> The way terrorism came up was in airport seizures. When someone would come in with a valise of money, at the time, screeners wouldn’t stop people, but they could notify us. If the passenger was on an outbound international plane, we’d wait. They’d close the plane, take away the walkway, and then we’d have them put it

[17] Siobhan O’Neil, "Terrorist Precursor Crimes: Issues and Options for Congress," (Congressional Research Service, 2007), 23.

[18] Ibid.

> back, board and say, “Is this yours?” We’d take the cash and put it in the general fund. There are bills, trust funds for each area—Social Security, transportation, and so forth.
>
> This was all pre-9/11. One of the things we noticed while we were doing airport seizures is that we found “negotiable instruments.” Those are demand deposits—a check is a good example. We were finding huge amounts of demand deposits, on flights to places like Singapore and Pakistan. We started looking at where it was coming from. It was charitable organizations, hotels, liquor stores. Hotels with zero occupancy. Who owned the hotels? Were they front companies? What were they doing? Laundering money from criminal pursuits. Some money, to some places, tips you off.

Following the money is done by an analyst who might be part of a fusion center, assigned to a task force, or part of a dedicated bureau at a number of federal agencies. Suspicious Activity Reports are a well-established practice in this arena. Investigations generally begin with suspicious transactions, which banks are required to report. There are many of these, and follow-up is often described as tedious, dull work. “Working financial crimes has always been an issue,” Jerome noted, “because it is not sexy.”

> There is what is called a “high-intensity financial crimes area” or HIFCA. We send our analysts to the meetings. What they are mainly doing is reviewing suspicious activity reports, SARs and Cash Transaction Reports, CTRs. For anything involving over $10,000, a CTR is required. Now, there could be no CTR, but the person in the bank identifies a suspicious trend in cash transactions. They will fill out a suspicious activity report. For example, people coming in doing multiple deposits of $9,999, keeping under the limit. Or having a business that wouldn’t quite generate over a million dollars or some extreme amount of money within a few weeks, and it just doesn’t look right to the person in the bank. They send all these SARs in, and the HIFCA collects them. And they give them out to the analysts to go through the information and process it, and see exactly, “OK, we’ve got this person with this business, is it possible they really are making the money with this business? Or do they have some type of income that would explain this amount of money going through their business or their account?” Analysts look into that, and then they put together a little profile of the person and the business, and see if these match. They try to see what previous transactions the person has done, if there are CTRs or SARS, to see if there is a pattern or a trend. At that point, the analyst goes and takes it to the HIFCA committee.

The procedures form a well-defined process for discerning a racket. It is perfectly legal to have cash transactions over $10,000. Deciding that something is amiss is a judgment the analyst makes, based on experience. She begins with a set of reports and evaluates if the activity could be explained by normal business practice. Information is compared with what the analyst considers to be non-criminal patterns. If it cannot be reasonably matched, she will look to see if it forms a known pattern of crime. Parts of the process, such as beginning from a lead and the prominence of human judgment, should be noted, because newer, computer-based types of analysis are critiqued for changes in these aspects.

Criminal funding of course does not go only through the regular financial system, to which Jerome ascribed “a number of problems tracking that money because they are very smart at moving it.”

> There are people body-packing [cash]. There are people shipping out what we used to call “the black market peso,” which is shipping out the product rather than cash. We have seen a number of terrorist groups that do that. It is easier to move, say, a clothing item or a high tech product out of the country than it is to move the equal value in cash. So they will move these items out and transfer them to other parts of the world as cash. And over there, they will be changed into an item that they can use, or they’ll purchase equipment. There are hawalas too that have been set up throughout the US, transmitting money. Along those lines, it is mainly this large network of support that we see and target here.

“We have this major problem,” Jerome elaborated, “where people are moving money, insane amounts of money in obvious scams. I wish I could give you some of the details on some of the things that they do.”

“Maybe there is something that was already in the news that you could talk about?” Jerome obliged with a commonly mentioned counterterrorism bugaboo.

> The charitable organizations, I’ll go into those. We had a number of charitable organizations that were operating throughout the country, for Muslim aid. Which I am all for—charity and people getting the support they need to—but the problem is you can’t differentiate a lot of times when the money goes over seas, how much goes to support the charity work and how much goes to support the terrorism work, which is ugly. And that is even more muddied by Hezbollah, because it is a large political group in Lebanon. They are funding hospitals and clinics and things we like to see funded, but a portion of that money they are sending is also going to support people buying missiles, buying bombs and training people. So it is one of those Catch-22s. You don’t want to stop these groups from doing legitimate charity work, but it is hard to slow them down.

The challenge with charities is that there is nothing illegal about fundraising itself. This is where the designation “foreign terrorist organization” becomes important. If the money can be connected to such an organization, the designation stands in for proving malfeasant motive and intent. Investigators have the basis for a case, and more tools at their disposal. The pattern of money flow does not reveal the crime, as it does for the suspicious activity reports. Rather, the money is a pathway investigators follow, which connects foreign terrorist organizations with domestic activities, and provides a site for intervention in the greater threat.

Ordinary Crimes

The link between crime and terrorism, from fraud schemes to cigarette smuggling, is generally accepted.[19] The assumption, also accepted but less supported, is that given state, local and tribal officers’ “existing skill sets, legal authority to investigate and

[19] Levitt and Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances."

prosecute such offenses, sheer numbers, and intimate familiarity with their jurisdictions,"[20] this nexus is the natural site for those groups to contribute. "Law enforcement and homeland security professionals," according to the Information Sharing Environment literature, are in "the unique, yet demanding, position of identifying suspicious activities, behavior or materials as a byproduct or secondary element to a criminal enforcement or investigation activity."[21] Frank, a thirty-year narcotics officer, was another deputy director at the fusion center. He was tasked with producing strategy and working papers, while Jerome focused on operational administration. When I interviewed Frank, he told me a story about a house call. The incident occurred years before, but epitomizes the kind of contribution to counterterrorism it is hoped law enforcement will make. "I went to a townhouse to try to find a runaway girl," he began.

> Her mother rang up saying her daughter was staying with this guy, who happened to be Iranian, but that has nothing to do with the story. She just rings up with this. We were concerned for the girl's safety, and her mother was concerned. She felt that this gentleman was maybe physically violent with her daughter. Her daughter was fifteen, fifteen or sixteen. So, we went to the house. We had been there previously on domestic violence. In those days, they were "family-type disputes," but were of a physical nature. So, we had some concern. We sent two officers and a sergeant. We went knocking on the door. The gentleman who opens the door was in his mid 30s. He opened the door, we explained to him why we were there, "we're looking for a runaway 15-year-old. He said, "Yeah, she's here. Come on in." So, we walked in the house and were going to try to get her to voluntarily go back to her mom's house. She was at a point where she was ready to do that. As we accompanied her out the house, we walked through the kitchen, which was open on both ends, and I walked behind, as the cover officer. I was walking behind this officer who is a real veteran. We walked pass the stove and he looked at the stove to see what the guy was cooking, I imagine, just a side glance. I looked and recognized that he was free basing cocaine on the stove. The other officer didn't recognize it. He just kept on going. And I said, "Sal, Sal! You see what he's doing here? He's cooking something." "I don't know what he's cooking." Sal had no experience in narcotics enforcement. So, we ultimately arrested this guy for possession of cocaine because he was freebasing right in front of us, or was preparing it.

"Why did he let you in?"

> It's amazing what people say yes to. I guess he thought he was all right, safe. If you think about, it fifty percent of us actually—I mean fifty percent of us who saw it—didn't recognize it and had no idea what it was. So, you know, he was just as lucky as he was unlucky. Unlucky won out because he ended up going to jail that night. But that goes to the training. If Sal had had more experience or training on what it looks like to free base cocaine, he might have made that same observation.

In this story, the cops were notified of the situation, which gave them cause to go to the house. The occupant invited them inside, giving them the right enter and observe. As it

[20] O'Neil, "Terrorist Precursor Crimes: Issues and Options for Congress," 23.

[21] "Information Sharing Environment (Ise) Functional Standard (Fs) Suspicious Activity Reporting (Sar) Version 1.5," ed. Program Manager for the Information Sharing Environment (PM-ISE) (Office of the Director of National Intelligence, 2009).

turned out, the man was arrested on a drug-related charge. The idea, however, is that regardless of the outcome of a service visit or criminal incident, alert officers are in position to see anything suspicious. Frank continued.

> In traditional law enforcement, he goes to jail. We write a report. It goes to the DA [District Attorney], where there might be a press release. That's it. And that may be all that's needed. But if there's a little bit more information to suggest that there might be a terrorism nexus—and I'm going beyond the fact that this guy happened to be Iranian, you know—perhaps some literature on the shelf that might have suggested a nexus to terrorism, anything like that. Where does that information go?
>
> Let's take a heightened level of education and training. How about: recognizing that the fact that he's got an under-aged female creates circumstances, but one of her concerns is "he says he is going to send me out of the country"? She really wanted to leave because he had been beating her. There could be human slavery involved here. OK, well, again, if you go to a larger perspective, is that a fundraising activity? Is there a nexus? Then there's his ancestry: does his nationality have some importance? I don't know. I'm not saying it does, but perhaps it does, or if it's even, "I can't tell," where does that information then go? Theoretically, it would go up through the organization to a terrorism early-warning group and it would come to us [the fusion center].

Frank illustrates common pro and con arguments for putting patrol officers in this counterterrorism role. Such service calls, not criminal investigations, are estimated to occupy four-fifths or more of patrol officers' time.[22] As conceptualized from the intelligence end, the man-hours consumed by service calls are advantageous. The time in contact with the community multiplied by the "sheer numbers" of cops make it more likely that they will happen upon the signs of pre-terrorism and foil a plot, disrupt the flow of money, or contribute intelligence about a larger terrorist network. For the suspicious activity report system, "peacekeeping" tasks are essential, although they are depreciated in a police hierarchy that rewards arrest statistics.[23] The disparity suggests that changes in fundamental police administration, already long and unsuccessfully prescribed, would be necessary for this part of the SAR component of the Information Sharing Environment to succeed.

Frank also mentions "literature on the shelf." The Functional Standards for the Information Sharing Environment admit that criminal organizations' "direct association with terrorism may be tenuous."[24] Cops' extolled "existing skill set" is built on patrol duties and in the course of criminal investigations, so skill at spotting ostensible indications of terrorism needs to be taught. Based on the counterterrorism trainings offered through the fusion center where I worked, which drew on Bureau of Justice Assistance sanctioned courses from around the nation, officers are taught an abbreviated history of terrorism, and a shallow, occasionally preposterous version of Islam. They are offered little or no

[22] Rubén G. Rumbaut and Egon Bittner, "Changing Conceptions of the Police Role: A Sociological Review " *Crime and Justice* 1(1979): 246.

[23] Peter Moskos, "The Better Part of Valor: Court-Overtime Pay as the Main Determinant for Discretionary Police Arrests," *Law Enforcement Executive Forum* 8, no. 3 (2008).

[24] "Information Sharing Environment (Ise) Functional Standard (Fs) Suspicious Activity Reporting (Sar) Version 1.5."

legal guidance on the civil liberties issues likely to arise. On the basis of these trainings, cops are asked to judge when possessing and reading religious pamphlets, a basic constitutional right, is suspicious. The emphasis, in the Functional Standards and in general police trainings, is on what Frank called “circumstances,” or technically, “attendant circumstances.”[25] One course I attended suggested always documenting the incident, and then letting a terrorism liaison officer decide if the information should be funneled into the ISE system. This problem is compounded when there is no criminal context.

Ordinary Behaviors. Field Contacts and Interviews

The three law enforcement counterterrorism tactics described so far are: following the money, identifying a link to terrorism in a criminal scheme, and being alert for signs in the regular course of duty. In these scenarios, police involvement is sanctioned, and there are protocols that take the weight of complete discretion off officers’ hands. The fourth counterterrorism tactic that Jerome brought up, and the most elemental piece of the information sharing environment initiative, is less defined and leaves assignation of guilt to an officer’s sense of the situation. Cops, in Jerome’s earlier description, are positioned to see “the people going out there and actually finding a good target.”

The first level of interaction with the public is variably called a field contact or field interview, depending on the nomenclature of the police or sheriff’s department. Filling out a Field Information, or FI, card is standard practice, not specific to counterterrorism operations. One cop who worked in a Northern California county sheriff’s office described it to me.

> Anytime you meet someone out in the field and you think you might run into them again, you would write up an FI card. Creating an incident would be the next level, and a report after that. An FI card would state that you had contact with so and so, when and how, if cooperative or not.

He added, “If you’re being written up on an FI card you are already suspect.” There could be something suspicious about the interaction. He gave the example of a parolee who failed to identify himself as such, and once, an old man down in a gully with a young boy.

> I want to check what his prior was for. It’s more of a moral judgment. If anything’s a little odd, I document it, if the kid makes a complaint three years from now, you now have enough for a case. That is a lot of the reason you take an FI card, people hanging around—just in case later, you do have a robbery.

There are regulations in place governing the interaction between a police officer and a member of the public. The nomenclature is not nationally standardized, but the categories are derived from federal judicial precedent, and are comparable. In a set of guidelines issued by a Texas police unit, for example, a “contact” is an encounter initiated by an officer in order to conduct an interview.[26] An “interview” means questioning a person who is not suspected of criminal activity. In many situations responding to the officer is voluntary (not, however, in a car). If the person refuses to answer, that refusal alone is not

[25] *Black's Law Dictionary*, ed. Bryan A. Garner, 8th ed. (St. Paul, MN: Thomson West, 2004).

[26] "Subject: Field Contacts, Number: 402/21," ed. State of Texas Alamo Community Colleges Police (2008).

enough for detention. An officer, though, has considerable leeway, as long as he or she is "able to point to specific suspicious conduct or circumstances that justify the detention." Examples of these elements which would assist an officer in justifying a stop and detention are:

> 1. The person is making evasive or furtive movements.
>
> 2. The person fits a wanted notice. (BOLO)[27]
>
> 3. The person is near the scene of a recently committed/reported crime.
>
> 4. The person's demeanor or presence is unusual for the time or the place.
>
> 5. The officer has received information that the person is involved in criminal activity.
>
> 6. In evaluating the person's conduct or appearance, an officer can rely on his training and experience to determine whether or not the person is a suspect. [28]

The only real restriction, as example six makes evident, is that the officer be "able to explain the reason why a person was detained and interrogated." As mentioned, the words used for these categories vary, and what the Texas unit called detention and interrogation would be a field interview (FI) in other regions. The requirements are the same.

> He does not need to point to any one thing that alone would justify his action but should refer to several things, each of which when taken alone may seem harmless, but when considered together by an officer who is trained or experienced in detecting criminal activity, raises a reasonable suspicion of a person's involvement in criminal activity.

An officer who initiates contact with someone in order to produce a Suspicious Activity Report is directed to follow these same guidelines.

An incident is the next level up in official reporting. "A call for service, any 911 call, takes some kind of documentation, even a 911 hang-up." The dispatcher perforce files them. The officer from the sheriff's department explained, "a dispatcher pulls up a name, and can see an incident and an FI card, both of these can be pulled up." As another cop told me, "All police work, if you can't write it, it didn't happen." If it is written, it becomes part of an archive. The archive is used to keep track of people, those who have committed crimes or (and this is the significant bridge) seem like they might commit crimes. These contacts between officers and the public, along with minor crimes, 911 calls, and overnight bookings are entered into computer databases as text, images, maps and other media, becoming "data" and the building blocks of homeland security's intelligence infrastructure. All of these tiny, actual events add up.

The definition of suspicious activity in the second published ISE guidelines was observed behavior that is "reasonably indicative of pre-operational planning related to terrorism or other criminal activity." One assumption here is that there are a series of

[27] "Be On The Look Out"

[28] "Subject: Field Contacts, Number: 402/21."

recognizable preparations preliminary to an attack. A second assumption is that the policing management system in place has officers regularly patrolling an area, so that they are familiar with it. This may or may not be the case, depending on which policing theory guides officer management at a local department.

The ISE functional directives provide criteria guidance for suspicious behaviors that should be documented. The first version provided an undifferentiated list. In response to criticism, a second version separated the behaviors into two categories, one of which was essentially criminal behavior that might also be related to terrorism, and the second of which was behavior that was noncriminal but might be related to terrorism: there's nothing wrong with looking at a bridge unless your goal is to blow it up. The first, "Defined Criminal Activity and Potential Terrorism Nexus Activity" included:

Breach/ Attempted Intrusion

Misrepresentation

Theft/ Loss/ Diversion

Cyber Attack

Sabotage/ Tampering/ Vandalism

Expressed or Implied Threat

Aviation Activity (in a manner reasonably suspicious or posing a threat)

The second category was "Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation."

Eliciting Information

Testing or Probing of Security

Photography

Observation/Surveillance

Materials Acquisition/ Storage

Acquisition of Expertise

Weapons Discovery

Sector-Specific Incident

The additional qualification was that these actions must be exhibited "in a manner that would arouse suspicion in a reasonable person". Addressing the complaints that had been made about the first version of the list which made no differentiation between criminal and noncriminal behaviors in terms of collecting and reporting information, a note was appended:

> These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that

> create suspicion (although these factors may used as specific suspect descriptions).

An ISE-SAR implementation project, in turn, developed a list of behaviors that officers on the street could use to code their reports. These attracted more attention than any aspect of the suspicious activity reporting before it, but before turning to them it is important to note that the shift to behaviors was in fact a response to criticisms about police profiling.

In 2003, the US Department of Justice issued policy guidance to federal agencies on racial profiling. The guidelines, instead of offering a definition of the act of racial profiling, defined it by the circumstances in which it is used.

> Use of race or ethnicity is permitted only when the federal officer is pursuing a specific lead concerning the identifying characteristics of persons involved in an *identified* criminal activity.[29]
>
> - The information must be relevant to the locality or time frame of the criminal activity;
> - The information must be trustworthy; and,
> - The information concerning identifying characteristics must be tied to a particular criminal incident, a particular criminal scheme, or a particular criminal organization.

The Fact Sheet then goes on, “federal law enforcement personnel must use every legitimate tool to prevent future attacks,” and so “race and ethnicity may be used in terrorist identification”.[30] The common elements, culled by one nonprofit police-monitoring group, characterize it as “mainly police-initiated action that relies, in whole or in part, on the race, ethnicity, or national origin rather than information regarding or the behavior of a person”.[31] While racial profiling may have been authorized in counterterrorism by a Bush administration justice department, there is no doubt that it is politically unacceptable to openly admit the practice.

The UK provides an interesting contrast case, in part because profiling is not prohibited. Lord Carlile, the government’s terrorism policy watchdog, even argued, “The police are perfectly entitled to stop people who fall within a terrorism profile even if it creates a racial imbalance, as long as it is not racist”. However, a study by the United Kingdom’s M15 found that “assumptions cannot be made about suspects based on skin colour, ethnic heritage or nationality" because "British-based terrorists are as ethnically diverse as the UK Muslim population, with individuals from Pakistani, Middle Eastern and Caucasian backgrounds”.[32] The UK’s Terrorism Act 2000, granted metropolitan cops the authority to “allow the police to search anyone in a designated area without suspicion that an offence has occurred”. In an ironic twist, police efforts to avoid allegations of prejudice

[29] "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," U.S. Department of Justice, http://www.usdoj.gov/crt/split/documents/guidance_on_race.php.

[30] Ibid.

[31] "Racial Profiling," *Police Assessment Resource Center* (2009).

[32] Alan Travis, "Mi5 Report Challenges Views on Terrorism in Britain," *Guardian*, 20 August 2008.

led to thousands of people being “stopped and searched by the police under their counter-terrorism powers simply to provide a racial balance in official statistics.”[33]

From Contacts and Incidents to Indicators

“You know about intelligence-led policing?” Jerome asked me. Intelligence-led policing was proposed in the early 1990s as a “conceptual model that used crime analysis and criminal intelligence in a strategic manner to determine offenders for targeting.” It is a general strategy of collecting and analyzing data in order to deploy resources, which might seem like common sense, but is in contrast to earlier and wide-spread belief in the effectiveness of guided police practice, such as randomized patrols (to surprise criminals).

> Crime reduction tactics concentrated on enforcement and the prevention of offender activity with a particular interest in using crime intelligence against the activities of prolific and serious offenders. Techniques included an expanded use of confidential informants, analysis of recorded crime and calls for service, surveillance of suspects, and offender interviews.[34]

Intelligence-led policing, only one among several police management strategies such as COMSTAT or Problem-Oriented Policing (POP), lends itself particularly well to integration with fusion centers and the Information Sharing Environment program. Although it is far from universally employed, the feature that Jerome mentioned, collecting pre-terrorism indicators, are available from any of the management models. The ISE-SAR program in Los Angeles has modified the basic form that patrol officers fill out so that they can check a box and send it to their Major Crimes Division. In smaller police agencies, the process is much more precarious. Ideally, information is passed to a terrorism liaison officer, or TLO, who is the point of contact to a larger geographically encompassing entity, such as a regional fusion center. The fusion center where I worked with Jerome and Frank was responsible for providing the training to officers who either volunteered or were directed to take the TLO position. Frank elaborated.

> We’ve got a terrorism liaison officer program. We give the officers training on how to identity terrorism-related crimes. The trainings are for what the TLO—the terrorism liaison officers—should be doing as far as the collection, dissemination of information and pushing it.

Implementation is not necessarily straightforward. Lieutenant Milton Nenneman, in the Sacramento Police Department, analyzed the program as deployed in his region around the California state capital. Some of the problems he found.

> An objective review of the program revealed several shortcomings. First, the TLO training was rolled out ahead of the TLO program itself. Secondly, agency administrators within the RTTAC [Regional Terrorism Threat Assessment Center]

[33] ———, "Terror Law Used to Stop Thousands 'Just to Balance Racial Statistics'," *Guardian*, 17 June 2009.

[34] Jerry H. Ratcliffe, "Intelligence-Led Policing," in *Environmental Criminology and Crime Analysis*, ed. Richard Wortley, Lorraine Mazerolle, and Sacha Rombouts (Portland, USA and Devon, UK: Willan Publishing, 2008).

> region were largely unaware of the program, did not know the benefits of the program or what the expectation for their participation might be, or, what level of commitment would be expected. Third, the training was announced via the normal training announcement system, and officers self-selected to go to the training without administrative support or time commitments. Fourth, what was not included in the curriculum was how the TLOs were to operate within their own agencies or in relation to the RTTAC. What had been done gave the officers a fine orientation on terrorism and then sent them back to their agencies without adequate support or operational instruction. According to Tim Johnstone, the RTTAC Commander, training had been provided to 475 TLOs without adequate forethought, as a knee jerk response to the need to provide and collect intelligence. A re-organization was in order.[35]

For everything to work, officers have to hear about the Terrorism Liaison Officer program and get trained. Their colleagues have to know to pass on the information to them. Frank was nonetheless ambitious.

> We feel this should be happening nationwide, state-wide, in our region. We really need to codify this push for trained TLOs, and put it down in writing. What should happen, what we're hoping to happen, is to have TLOs be able to go out and do follow-up investigations. Because now, we can only do so much. We can set the framework but you actually need to have field agents that are out there knocking on doors, or sitting and watching, doing surveillance on people, seeing what their business is like.

Jerome, as well, emphasized the importance of the TLOs and providing adequate training.

> There's many other factors, many opportunities that people exploit to make money that these guys can identify. There is this whole issue of Middle Eastern organized crime as far as Middle Eastern terrorism but there's other groups. People focus on them a lot, and I know I do a lot, just because of my background, but we have Abu Sayyaf, which is Philippino. We have Sri Lankan groups, Tamil Tigers in our area. And we also have converted extremist black Muslims, who are in our area, who all have the same goal of a jihad, a literal war, a physical war against the United States and the infidels. So we have all these groups out there and we're trying to get the TLOs a broad knowledge base, and trained, to being able to share the information.

Regardless of the match between ideal and implementation, the question is if this kind of day-to-day surveillance catches terrorists. It produces large amount of data, of which both the collection and processing occupy man-hours that could be otherwise spent. Another question is if *requiring* officers to report suspicious activities changes the dynamic of their public presence. For Jerome, it only made sense:

> There are requirements about domestic violence. Shouldn't we have the same requirements about terrorism investigations? Shouldn't they have the same priority? I think it is a serious matter that a spouse abuses another spouse. There

[35] Milton Nenneman, "An Examination of State and Local Fusion Centers and Data Collection Methods " (Naval Postgraduate School, 2008), 79.

> are reporting requirements on that. If an officer believes that there is a suspicious incident, maybe related to terrorism, and that's something he's trained in, shouldn't we have the same requirement of reporting? But we don't. There is no reporting requirement on suspicious activities. There's no penalty on people [LE] not telling us or giving us the information. I think there should be. I think that agencies should be willing to give that information in the first place, but if there's no requirement, people—especially cops—think "if you're not required to do it, why do it"?

Law enforcement is overworked as it is, I pointed out, quoting any or possibly all of my co-workers. "How does this fit in, giving them another task"? Jerome looked intent, and then chuckled:

> I think it only adds to what they're doing as far as law enforcement officers but you're right, that does come up. I remember, one of our CHP [California Highway Patrol] officers who was doing terrorism liaison officer training to his own people. He was going out to the CHP, telling them the things to look for, what to see, what to report to them, so we could collocate all this information in the system. He was handing his cards out to people, and he got back up to the podium. An old crusty guy, who was an older gentlemen, a CHP officer, from the back of the room walked up to him, and threw his card down, said "I don't need that", and walked back. They got into it. Basically, he goes, "I got enough to do, I don't need to do terrorism stuff too. That's your job."

The little-discussed risk is that a dynamic is set up, in which law enforcement, seeking terrorism, find what they seek. Ordinary criminals are fit to the mold of terrorists. The statement that terrorism is too facilely identified is supported by criticisms that a low percentage of investigations have led to prosecutions, fewer have been successfully prosecuted as terrorism, and, of those, not all withstand scrutiny.[36] This aggravates a common, although not ubiquitous, mindset among cops that as long as "bad guys" are being caught and punished, it makes no difference. In an interview, former 9/11 Commission Co-Chair Thomas Kean commented.

> [Y]ou can't say there couldn't be threats, traditional threats, from all sorts of sources within the country, going to the Haymarket explosion in Chicago back two centuries ago. We've had anarchists; we've had people trying to do harm for one reason or another.[37]

His point, however, is that they were not al-Qaeda.

> What we're talking about here is a specific organization that's now around the world in its scope, that has announced they want to do us harm and kill as many Americans as possible; that has technology to support them and has some very intelligent people. ... That is the enemy, and that is who we're fighting, and we've got to always keep our focus on that.

The lack of al-Qaeda ties however, may be what makes these cases attractive for prosecution, as they suffice to show results, but are lacking in greater value intelligence

[36] Scott Shane and Lowell Bergman, "Contained? Adding up the Ounces of Prevention," *New York Times*, 10 September 2006.

[37] Thomas Kean, "Interview," *Frontline PBS*, 27 March 2006.

that would be lost in a prosecution. “Homegrown terrorists” in a US court are legally the same as any member of a major international terrorist group. In fact, they may have a connection to such a group, but if those in the news are indicative, they are operationally self-directed.

In 2005, Kevin James and three converts to his prison Islam group, Jamiyyat Ul-Islam Is-Saheeh (JIS), were indicted in California. Their case, in which noticing “suspicious literature” played a part, became known as the Los Angeles bomb plots. Shortly after the last sentencing in 2009, former Los Angeles Chief of Police William Bratton pointed to it as an example of police excellence.

> We have thwarted some terrorist attempts in Los Angeles just by good, basic police work. There were a couple of guys holding up gas stations and convenience stores. One of the neighboring police departments, aware of that, set up a stakeout and caught the guys robbing the convenience store. But the detectives then did what good detectives do—they did roll-back warrants, meaning they went back to the residences where these guys lived to see if there was additional evidence that could be used in proving some earlier crimes. During one of those, they found material in Arabic. One of the detectives, who had been trained in counterterrorism, passed the material up to the Joint Terrorism Task Force, and what we uncovered was a plot that had been hatched by an imam [James] in prison to attack US Army recruiting stations and Jewish places of worship here in Los Angeles. So if these characters had not been detected with the basic prevention of the holdup, who knows, six months down the line they might have gone ahead with their plan.[38]

Chief Bratton’s description contained all the basic elements of the domestic version of the crime-terrorism link, and the “enemy within” phenomenon. Like the terrorist shoe-bomber Richard Reid and Jose Padilla, who was held as an enemy combatant, Jamiyyat Ul-Islam Is-Saheeh was identified as part of a worrisome trend towards prison radicalization. Since black men make up a disproportionate percentage of the prison population, this puts them in the historically familiar position of being a threat. Like the 2006 “Sears Tower Plot,” which involved a group of Islamic converts in Miami’s Haitian community, or that of Syed Haris Ahmed and Ehsanul Sadequee, youths from Atlanta, Georgia, the JIS group in Los Angeles was not directed by al-Qaeda or any affiliate, but acted on its own.[39]

The JIS counter-operation enacted the Department of Justice’s strategy of aggressively pursuing “terrorism-related” cases and closing in before imminent danger.

> The fuse that leads to an explosion of violence may be long, but once it is lit—once individuals unlawfully agree to support terrorist acts at home or abroad—we will prosecute them to snuff that fuse out.[40]

The noteworthy point is that wrong-doing occurs in “agreeing to support terrorist acts.” As a result, plotters may be arrested and prosecuted before it becomes completely clear if they would ever have carried the plan to fruition. One of the reasons that JIS became

[38] Robert Maxwell, "Chief Bratton and Jim Wiatt: Friends Help L.A.’S Top Lawman Keep This City Safe," *Los Angeles Times*, 7 June 2009.

[39] Shane and Bergman, "Contained? Adding up the Ounces of Prevention."

[40] Bill Rankin, "Ex-Tech Student Found Guilty on Terrorism Charge. Father: Ahmed ‘Not Guilty of Any Crimes in the Eyes of Allah’," *Atlanta Journal-Constitution* 2009.

such a poster child was that there was fair certainty that they would go through with it. Not only had the outside men committed open-and-shut crimes, but they also named targets, wrote a provisional press release, and acquired firearms. James, who never left the prison, claimed that he did not found a radical Islamic group inside, and denied that the perpetrators had pledged loyalty to him. Nonetheless, he pled guilty to conspiracy to levy war against the government of the United States through terrorism, and to oppose by force the authority of the United States government. The others, except for one deemed mentally unfit to stand trial and sent to undergo psychiatric treatment, were also charged with conspiracy to possess and discharge firearms.

Other cases are not always as neatly tied to crime, or as far along. The “Sears Tower Plot, by the Miami men, was described by terrorism expert Marc Sageman as “nonsense.” The *New York Times* wrote, “the FBI itself supplied Al Qaeda. Its informer, posing as a member of Al Qaeda, bought the men military boots and promised money and weapons even as the group began to crumble.”[41] In Atlanta, Georgia, Sayed Haris Ahmed was found guilty of conspiring to provide material support to terrorists in the US and overseas. Although the youth and his partner met with “suspected terrorists” in Toronto and made amateur videos in Washington, DC, sent abroad to show they could get close to targets, his family believed that he “never would have followed through on any plans to engage in terrorism.”[42] “His only crime,” they claimed, “was ideas.”[43] Ahmed’s attorney argued that he “was an immature college student who had ‘momentary ideas, childish fantasies’ that were never carried out.”[44] He traveled to Pakistan to join a terrorist training camp, but changed his mind and reenrolled at Georgia Tech. Yet, aggressive prosecution of these sorts of cases is what the government and some counterterrorism experts argue has kept the US from experiencing another major attack since September 11th. “This investigation is connected to arrests and convictions of multiple terrorist supporters in Atlanta and around the world,” claimed a US attorney about Ahmed and Sadequee, “all before any innocent people were killed.”[45]

These cases gathered together represent the effects of an explicit shift in the Department of Justice’s approach to counterterrorism strategy. In its 2001 report, the Department of Justice’s published number one goal was to “protect America from terrorism.” After 2003, that goal became prevention.[46] The top-down policy change filtered through the criminal justice system. The guidelines for implementing the Suspicious Activity Reporting program is one manifestation. The way cases such as these were prosecuted is another. The transition to prevention-oriented prosecutorial policies was enacted through a series of methods.[47]

One sign is the increased use of the charge of “seditious conspiracy”, which was used against the 1993 World Trade Center bombers, and the Los Angeles plotters With

[41] Shane and Bergman, "Contained? Adding up the Ounces of Prevention."

[42] Rankin, "Ex-Tech Student Found Guilty on Terrorism Charge. Father: Ahmed ‘Not Guilty of Any Crimes in the Eyes of Allah’."

[43] Bill Rankin, "Terror Trial Verdict: Guilty," *Atlanta Journal-Constitution* 2009.

[44] Ibid.

[45] Rankin, "Ex-Tech Student Found Guilty on Terrorism Charge. Father: Ahmed ‘Not Guilty of Any Crimes in the Eyes of Allah’."

[46] John Ashcroft, "Fy 2003 Performance & Accountability Report," ed. Department of Justice (Washington, DC: Office of the Attorney General 2004).

[47] Robert Chesney, "Federal Prosecution of Terrorism-Related Offenses: Conviction and Sentencing Data in Light of The "Soft Sentence" And "Data Reliability" Critiques," *Lewis & Clark Law Review* (2007): 854.

roots in the 1798 Sedition Act, it allows the government "to charge people who plan but do not carry out crimes against the United States."[48] The initial precedent was the requirement of a clear and present danger to rights the government lawfully protects. The assumption that these acts constitute such a danger is the fulcrum of the shift. Before, law enforcement might have waited for evidence that a plot would be carried out. Ahmed did, after all, turn back after making it to Pakistan. Now, evidence of the plot is enough. The pivotal judgment in these situations is whether someone will turn a violent fantasy into reality. There is no disagreement about what Ahmed did. In Ahmed's case, there was much proof of the fantasy. He wrote about engaging in jihad, met with shadowy people in another country (Canada), filmed national landmarks as targets. In a chain of truth claims and corresponding jurisdictional consequences that repeats in the counterterrorism efforts to be discussed, the fantasy was accepted as proof of a plan "to provide terrorist support," which was accepted as proof of future action.

The US had antiterrorism laws before 2001. Legislation such as the Patriot Act gave law enforcement more authority and resources in pursuing investigations, created some new crimes, and increased penalties for others. Yet, especially for the examples discussed here, what can be seen is more a change in tolerance and tactics than law.

Discernment and Discretion

There has been a ludicrous, in some ways alarming uptick in aggressive police control of photos taken "with no apparent esthetic value."[49] Oppressive to those snared,[50] and unlikely to have a chilling effect of the production of bad pictures, the tactic has also served to make a mockery of the police. Because the illustration is exactly that of an artistic evaluation, politely understood to be an opinion that cannot be wrong, it highlights the delicacy of the decision given over to the street patrol officer in suspicious activity reporting. While the stories of cameras confiscated from photographers on art project shoots or class assignments make it seem obvious that the police exercised stereotypically poor taste (in a word association train that goes police…totalitarian…gigantically tasteless stone statues of rulers), there is another, subtle issue in play. The responsibility for discerning that an action is out of place lies with the officer. There is no reasonable and certainly no politically correct way to describe this threat at the level of a person on the street. Purely racial or ethnic or religious profiling is not legal nor has it been shown to work.

Public officials were confronted on 9/11 with the terrifying dilemma that "terrorist" behavior could overlap with ordinary behavior in every way except for motive and intent. Suspicious activity reporting, followed by vetting at a fusion center, analysis and further evaluation in conjunction with data from the wider intelligence network tackled the problem

[48] TITLE 18 > PART I > CHAPTER 115 > § 2384 "If two or more persons in any State or Territory, or in any place subject to the jurisdiction of the United States, conspire to overthrow, put down, or to destroy by force the Government of the United States, or to levy war against them, or to oppose by force the authority thereof, or by force to prevent, hinder, or delay the execution of any law of the United States, or by force to seize, take, or possess any property of the United States contrary to the authority thereof, they shall each be fined under this title or imprisoned not more than twenty years, or both." Rob Harris, "The Enemy Within: Kevin James and the Jis Conspiracy " *Frontline PBS* 2006.

[49] "Findings and Recommendations of the Suspicious Activity Report (Sar) Support and Implementation Project," (Bureau of Justice Assistance, 2008), 43.

[50] Eric Schmitt, "Surveillance Effort Draws Civil Liberties Concern," *New York Times*, 29 April 2009.

thus perceived. To grasp what was otherwise intangible, this new apparatus was developed. Yet, the process put a perhaps impossible task in the hands of street cops. The foundations of the intelligence architecture are the presumed capabilities of the police to discern suspicious activities. Their “gut instinct” is privileged while simultaneously defined as insufficient, the discrepancy to be made up with, first, clear guidelines and second, training. One of those guidelines, issued to the Los Angeles Police Department, was to be aware of photography with no apparent aesthetic value. Outcry greeted the publication of the list and, on the federal level, new functional standards specified, “Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person.”[51]

The issue raised is if the police’s capability for discernment is not irrevocably delegitimized by the socioeconomic, racial, gender and other life lenses that everyone acquires, further distorted by a prejudice stereotypically assigned to the cop role. The closest parallel to the critique of impartiality seemingly required in suspicious activity reporting has been explored in the idea of discretion, “an officer’s decision to act or not act when there is an option to do otherwise.”[52] Discretion was reputedly “discovered” by the legal community in the 1960s, but of course has been part of practice for at least as long as the word “police” can be understood to refer to more or less the same concept.[53] Peter Moskos, a professor of Criminology and former police, provides a succinct history of the research.

> Overall, the literature establishes that police exercise considerable discretion in their day-to-day arrest decisions. While such discretion was initially seen as prima facie evidence of racism and something to be identified and eliminated, most contemporary research tends to see police discretion as inevitable and even desirable when used judiciously.[54]

The idea that the law was not evenly applied to everyone could not seriously have been shocking at any point in history. The outrage must have been in many ways performative, but to be sure, rooted in the assumption that the inequality was systematically applied against certain groups, such as people of color or those living in high-crime neighborhoods. A positive valence of discretion came about from research showing that selective use of the law was sometimes a tool of peace-keeping.[55] Cops might turn a blind eye to social public drinking during hot summer nights in apartment housing projects. To enforce the law, in the absence of rowdiness or noise, would be to refuse the inhabitants the enjoyment of their only public space, the stoop that served as front yard and town square. Other research confirmed that socioeconomic status of the neighborhood, “situational variables such as the demographic characteristics of an officer, the victim’s cooperativeness, the victim’s injuries, and the time of shift” all affected police discretion. Moskos’ own research pointed to “police officers’ desire for court and overtime pay as the main variable affecting quantity of low-level discretionary arrests.”[56]

[51] "Information Sharing Environment (Ise) Functional Standard (Fs) Suspicious Activity Reporting (Sar) Version 1.5."
[52] Moskos, "The Better Part of Valor: Court-Overtime Pay as the Main Determinant for Discretionary Police Arrests."
[53] Ibid.
[54] Ibid.
[55] Rumbaut and Bittner, "Changing Conceptions of the Police Role: A Sociological Review ".
[56] Moskos, "The Better Part of Valor: Court-Overtime Pay as the Main Determinant for

> Frank shared his ideal of discretion.
>
> I'll tell you about one of the proudest moments in my life. There was this time where I was followed into the parking lot on a uniform patrol by a guy. As I drove around on a Sunday morning, he followed me in the car and I was getting increasingly concerned. If I stopped, then he stopped and if I moved, he moved. I finally got out of my car, figuring "this is going to be bad, whatever it is". And he said…opened his car door and yelled at me, "You're Officer May, right?" And I said "Yeah!" I'm snapping my gun. It looked really bad. I think he's tossing the anger towards me, and he says, "I've been looking for you for a couple of years! You probably don't remember me but you stopped me one night when I was a drunk driver. You arrested me and my life was pretty close to being at an end. I was getting a divorce. My family was destroyed. I have small kids and when you searched me, I had dope in my pocket. You lectured me, and you destroyed the dope right on the scene, and said that I would have enough problems doing the drunk driving and it was my option. You said to deal with the drunk driving. You said I can go get more dope, and continue to watch my life go down the toilet and lose my kids, or I can turn around and I would have lots of times to think about it. I was drunk at the jail. And I did, and you made a difference of my life and I've been looking for you for over two and a half years to thank you.

Like most cops, Frank viewed himself as a public servant—not necessarily a good one, but with a chosen vocation nonetheless. Domestic surveillance did not strike him as sinister, because he understood law enforcement as the "good guys." A less rosy view of discretion, or the officer's ability to apply it, is epitomized by the congressional testimony of constitutional and international law lawyer Bruce Fein.

> Core First Amendment principles will never be honored by law enforcement officers or public officials. Their psychological preoccupations are order and the status quo; they viscerally fear or are perturbed by the prospect of change or challenges to the existing power structure. Further, they are rewarded financially and professionally by the volume of intelligence collected. There are no serious quality controls because few if any are fit to separate the terrorist wheat from the innocuous chaff.

Fein skips racism or other common accusations against law enforcement and their application of discretion. He bases his indictment of counterterrorism surveillance on a more general indictment of law enforcement and politicians. His point is that it is not in the self-interest of those in power to support First Amendment principles, presumably because he believes that the free exercise of religion, the press and speech will lead to change. He implicitly dismisses that training or regulation as useful restraints on abuse, in a leap of logic over why, with officers' alleged preoccupation with the rules, they would not be similarly fixated on honoring core First Amendment principles. Alternatively, he assumes that the First Amendment would not activate their rigid allegiance to order and the status quo.

The LAPD list was critiqued as the wrong guidance for cops, especially given that Fein's view of the police is widespread. In reporting, experiential knowledge and skill at discretion is both privileged and assumed to require specific training for a new threat.

Discretionary Police Arrests."

Frank, cognizant of such fears and suspicious behaviors' delicate relationship to First Amendment rights, repeated to me, "We have to educate them. Training is one of the things we do to try to develop people so that they can identify terrorism-related crimes." The list of suspicious behaviors does not mean that all actions are suspect. However, those behaviors defined as having the potential to be suspicious present no exclusively distinguishing diacritic. This suggests that any unmarked action could also be suspicious. The list might subtly criminalize one set of behaviors, while obscuring others, or narrow officer attention so that genuinely suspicious behaviors go unnoticed. Although it was probably not conceptualized this way, the list can more accurately be seen as a way to remind officers to simply pay attention: a technique for maintaining vigilance.

The Seamless Network

At one point, I asked Frank, "Where would the intelligence come from? The police on the street?"

> It will come from a cellular network of people who developed multidisciplinary relationships, so all first responders.

Not just police?

> Not just police. The public would go to their local first responders whoever it is, be it fire service, medical service, law enforcement, for whatever their needs are. Those first responders would be networked together. They would supply the underlying information that becomes intelligence. Terrorists, they've got to have a network that is familiar with how to get around here, where to put them up, set them up, before they actually get to their operation. Here [at the fusion center], we get the training out to these folks who become our reporters basically, and call us, push the information to us. That is one of our main resources. We are getting these guys to supply us with the information on what they are seeing.

For cops who view themselves as working in a committed way towards the security of the public, everyone should be behind this effort, and certainly firemen as well. The idea that firemen gathering up terrorist tips for an intelligence fusion center could be too much surveillance did not come up. One retired cop, when I suggested this might be viewed negatively by some, told me, "If they have nothing to hide, they have nothing to fear." For example, Lieutenant Nenneman wrote an information-packed masters thesis on fusion centers. In concluding that greater participation on the part of the entire emergency response community must be encouraged, he unselfconsciously offered, "The ER community, particularly the non law enforcement community, needs to recognize that forwarding a tip is not an indictment, and that no onus is attached if an observation turns out to be merely innocent behavior."[57]

Despite Fein's assertions, in the period of heightened fear after the quite real terrorist attack of September 11th, many public officials acted in good faith to develop an apparatus to deal with an apparent threat. Since it rapidly became known that some of the

[57] Nenneman, "An Examination of State and Local Fusion Centers and Data Collection Methods ", 74.

data that could have prevented the attacks had been in hand, it made sense to mandate that there be technological means and procedural standardization for all segments of the US government to communicate. Yet it is an additional and not self-evident step to enlist state, local and tribal police as a ground-level social surveillance force. The point that both advocates and opponents make is that there are 780,000 sworn state and local law enforcement officers in the United States. As the war on terror geared up 2002, Giorgio Agamben advised, “When politics… reduces itself to police, the difference between state and terrorism threatens to disappear. In the end it may lead to security and terrorism forming a single deadly system in which they mutually justify and legitimate each others' actions.”[58] Using the police in dubious counterterrorism activities, he suggests, risks fundamentally compromising the legitimacy of the state. Yet state, local, and tribal law enforcement were enlisted in an on-the-ground national intelligence force, with remarkably little notice.

The legal basis can be traced back to the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Significant documents, including the earlier Patriot Act, the 2004 9/11 Commission Report, and executive orders issued in response, developed the reasoning underlying the Intelligence Reform Act. The Patriot Act, determined to legally remove the largely cultural or habitual "wall" between intelligence and law enforcement, explicitly encouraged cooperation. The 9/11 Report identified resistance to sharing information as "the biggest impediment to...connecting the dots."[59] The President followed on this with an executive order on “Sharing terrorism information to protect Americans,” which mentioned and included state and local law enforcement. Then, the Intelligence Reform and Terrorism Prevention Act, Section 1016, ordered the creation of the Information Sharing Environment, to be run by a presidentially appointed Program Manager. While both the National Strategy for Information Sharing, and the Fusion Center Guidelines in 2005 emphasized the reporting of “information of intelligence value from state, local, and tribal law enforcement entities and private sector stakeholders,” the fusion centers guidelines pushed considerably closer to the subsequent ISE plan.[60]

> One of the principal outcomes should be the identification of terrorism-related leads—in other words, any “nexus” between crime-related and other information collected by local, state, and private entities and a terrorist organization and/or attack…

Some of the recommended goals and functions for fusion centers include the following:

> Serve as a receipt-and-dissemination hub for law enforcement information provided by federal entities…
>
> Serve as the initial point of contact for the public and private sector personnel to report suspicious circumstances or threat-related information.
>
> It is recommended that all investigative or intelligence personnel, as well as nontraditional collectors of intelligence such as fire, emergency management, and

[58] Giorgio Agamben, "Security and Terror," *Theory and Event* 5, no. 4 (2002).

[59] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 416.

[60] "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World. Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal, and Federal Level. Law Enforcement Intelligence Component," ed. Department of Justice (2005).

> health personnel, receive awareness training. Personnel should be equipped to identify suspicious activities or threats and provide information to fusion center personnel, as appropriate. (67)

Real specificity, however, began with the guidelines developed by the office of the Program Manager. In January of 2008, the Information Sharing Environment program issued its first "functional standards" for reporting suspicious activities, containing a description of the process and definitions. The ACLU, already tuned-in to fusion centers, began a review. In spring of that year, as group of representatives from state, local and federal agencies began work on an implementation project. This group made site visits to police departments in Chicago, Los Angeles, Boston and Miami. The report they produced in October contained the Los Angeles adaptation of the ISE Functional Standards that finally made the news media notice.

Up to that point, the Information Sharing Environment plan and its implementation had attracted little attention. This was at least partially because the major news media appeared to understand it as part of a technology subgenre, and missed the importance to regular policing, more clearly a mainstream issue. Federal Computer Week's Ben Bain was the only writer to cogently report on the ISE and SAR process. Reports on fusion centers and inadequate protection of civil liberties from the American Civil Liberties Union, the *New York Times*, *Washington Post, Boston Globe* or elsewhere were more common, but almost never connected with the Information Sharing Environment by name.

Vigilance, Surveillance and the Dangerous Individual

Vigilance “the action or state of keeping careful watch for possible danger or difficulties”[61] comes from Latin *vigilare*. Surveillance, with the same root word, means “close observation, esp. of a suspected spy or criminal.” The difference is that of subject and object. Vigilance is a subject's state, in relation to an environment, while surveillance is an action the subject takes, that of focusing attention on a suspicious person. Vigilance is the mode of subjectification both required and produced by surveillance. As Nicholas Langlitz observed in another context.

> In order to work, vigilance requires the cooperation of the citizenry: a self-observation of and by the population. This, in turn, requires the formation of vigilance as a mode of subjectivity, which is inseparable from the formation of individual responsibility. Advanced liberal regimes require such internalizations of their political rationalities to govern their citizens at a distance.[62]

To some extent, since 9/11 the US population has been asked to become vigilant. Citizens are asked to remain to alert, to report suspicious people or packages. There was a vocal minority that extorted Americans to feel that they were at war, to engage them in the existential battle. Even through the nation was in fact at war, in more than one country, the effort was not transformative. Mass surveillance of and by the population never

[61] *The New Oxford American Dictionary*.

[62] Nicolas Langlitz, "Pharmacovigilance and Post-Black Market Surveillance," *Social Studies of Science* 39, no. 3 (2009): 397.

reached the kind of diffusion found, for example, in the United Kingdom. Instead, in the United States, the subjectification imposed by the SAR system is largely focused on the police. Cops are traditionally supposed to be vigilant for suspicious behavior, and the SAR process transforms what were heterogeneous pieces of information—freehand descriptions, subjective selection of important details—into standardized dots that can be cumulative and exchangeable. However, is there a difference between facilitating the reporting of terrorism and mandating it? Is there a difference in shifting from the traditional police role of vigilance to one of surveillance?

In these terms, the SAR process, perhaps accidentally, forces the officer to make this shift. Here, Michel Foucault's discussion of the dangerous individual is germane.

> Legal justice today has at least as much to do with criminals as with crimes. Or, more precisely, though for a long time the criminal had been no more than the person to whom a crime could be attributed and who could therefore be punished, today the crime tends to be no more than the event that signals the existence of a dangerous element—that is, more or less dangerous—in the social body.[63]

Crime passed from being a transgression to an indicator.[64] In the SAR-ISE system, suspicious activities are parallel to crimes. They signal the existence of a dangerous element. Of course, the problem is that many of the behaviors listed in the ISE functional standards and by the Los Angeles Police Department are also ordinary behaviors. The officer is presented with a paradox.

> For the modern system of sanctions—most striking since Beccaria—gives society a claim to individuals only because of what they do. Only an act, defined by law as an infraction, can result in a sanction, modifiable of course according to the circumstances or the intentions. But by bringing increasingly to the fore not only the criminal as author of the act, but also the dangerous individual as potential source of acts, does not one give society right over the individual based on what he is?... what he is by nature, according to his constitution , character traits, or his pathological variables.

Intention becomes everything. Cesare Beccaria, the Italian reformer whose short treatise *On Crimes and Punishment* swept the world, tried to refuse any element of intention. Crimes, he argued in 1783, "are only to be measured by the injury done to society."[65]

> They err…who imagine that a crime is greater or less according to the intention of the person by whom it is committed; for this will depend on the actual impression of objects on the senses, and on the previous disposition of the mind; both which will vary in different persons, and even in the same person at different times according to the succession of ideas, passions, and circumstances. Upon that system it would be necessary to form, not only a particular code for every individual, but a new penal law for every crime.

[63] Michel Foucault, "About the Concept of The "Dangerous Individual" In Nineteenth-Century Legal Psychiatry," in *Power: Essential Works of Foucault 1954-1984*, ed. James D. Faubion (New York: The New Press, 2000).

[64] Nicole Hahn Rafter, *Creating Born Criminals* (Urbana: University of Illinois Press, 1997), 2.

[65] Cesare Beccaria, "On Crimes and Punishments," (Liberty Library of Constitutional Classics 1819 (1764)).

The problem then shifts to an evaluation of the individual, to a sense of his or her motive and intent. This rests on the discretion of the officer. Somehow the police have to judge what the person does, not who the person is, but the action is innocuous except in relation to its obscure purpose. The officer is instructed to pay attention to the totality of circumstances, to the environment.

The formulators of the system are not unaware of this issue, for which there is no definitive solution. Instead they move the debate by countering that no sanctions are being imposed, and it is to this locus of truth claims that the argument shifts. "If you've done nothing wrong, you've nothing to worry about." Is harm done to an individual by mention in a field contact or incident? *Time* magazine, hardly open to the accusation of overly liberal polemics that plague the ACLU, reported that "in 2005 and 2006 undercover members of the Maryland State Police had carried out surveillance of war protesters and death penalty opponents."[66] They entered "the names and personal information of 53 peaceful left-wing activists" [67] into the Maryland fusion center's database and the Washington-Baltimore High Intensity Drug Trafficking Area database, which possibly were shared with the National Security Agency.

The procedures for including data in the Information Sharing Environment were modified to tighten the vetting system between the first and second version of the ISE functional standards. An SAR might come directly from a local precinct, but then goes through a two-step process.

> First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism.[68]

This change was made following the recommendation of privacy advocates, including the ACLU, but is of course no guarantee. How were the lives of people on such lists affected? The Maryland state police claimed that none of the protesters were entered into the official federal terrorist watch list, which has well-known consequences in the form of travel inconveniences, or even restrictions. Historically such lists have affected employment, housing and other aspects of life. There is also of course the problem of inaccurate data for computer analysis that relies on links between people, or "learns" based on the data that are input, and it is to this problem of how the dots are connected that we turn next.

The Suspicious Activity Report project was thoughtfully designed and implemented, with feedback mechanisms and actual change resulting from the input of concerned public parties. For some the attention to detail may have been only a way to keep it under the media radar but for others, this was a sincere attempt to create a system that would maximally keep Americans safe with minimal invasion of privacy. This is cold comfort if the whole apparatus of surveillance strikes one as sinister, as is the fact that the single greatest impediment to its function is that no cop in his or her right mind wants the

[66] Hilary Hylton, "Fusion Centers: Giving Cops Too Much Information?," *Time Magazine*, 9 March 2009.

[67] Robert Baer, "When the State Police Fingers Terrorists," *Time Magazine*, 17 October 2008.

[68] "Information Sharing Environment (Ise) Functional Standard (Fs) Suspicious Activity Reporting (Sar) Version 1.5."

added work, bureaucracy, and time away from career-relevant arrests, unless there is a very clear and present danger to the security of the community.

Chapter Seven. Connecting the Dots

"A 'smart' government would *integrate* all sources of information to see the enemy as a whole," asserted the 9/11 Commission Report in 2004.[1] "Integrated all-source analysis," it continued, "should also inform and shape strategies to collect more intelligence." Otherwise, "it is not possible to 'connect the dots.'"[2] This sequence of claims would push the spontaneous participation of state and local law enforcement in counterterrorism begun in 2001 into congressionally approved law by 2007. By July of 2008, the American Civil Liberties Union (ACLU) was issuing warnings about domestic intelligence and fusion centers:

> Overall, it is becoming increasingly clear that fusion centers are part of a new domestic intelligence apparatus. The elements of this nascent domestic surveillance system include:
>
> Watching and recording the everyday activities of an ever-growing list of individuals
>
> Channeling the flow of the resulting reports into a centralized security agency
>
> Sifting through ("data mining") these reports and databases with computers to identify individuals for closer scrutiny
>
> Such a system, if allowed to permeate our society, would be nothing less than the creation of a total surveillance society. Recent reports have confirmed each of these elements.[3]

There were between 50 and 60 fusion centers in the United States at the time of the ACLU publication. A year later there were 72.[4] The first centers began as state responses to 9/11. Local leaders, as Jerome, the deputy director of the fusion center where I did research described it, felt keenly that they were responsible, and would be held answerable, for the safety of their constituents. The attacks proved to them that the federal government could not be counted on to ensure security, or to share the necessary information for local government to compensate. The early centers grew out of existing police intelligence and analysis units; some had been single-issue task forces within larger police departments, while others had existed as independent agencies, often a High Intensity Drug Trafficking Area program site (the HIDTAs). They did not necessarily have experience producing strategic intelligence and planning. Most, however, already provided operational and/or administrative support to their base by sponsoring task force meetings for gangs or narcotics trafficking, and lending equipment and analytical staff. Legal

[1] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 401.
[2] Ibid., 408.
[3] Mike German and Jay Stanley, "Fusion Center Update," (American Civil Liberties Union, 2008).
[4] As of July 2009. "State and Local Fusion Centers," (Washington, D.C.: Department of Homeland Security, 2009). http://www.dhs.gov/files/programs/gc_1156877184684.shtm

authority for the first fusion centers was cobbled together from their existing statutes and from memorandums of understanding with new partners.

The federal government took notice of the initial wave of start-ups as they emerged, around 2003, and fusion centers began appearing in federal discussions of strategies for the new "homeland security." Some fiscal support was offered beginning in 2004 through a DHS Grant program. Members of the Department of Justice's Global Justice Information Sharing Initiative and the Homeland Security Advisory Council started developing guidelines, together with representatives culled from law enforcement agencies across the US.[5] In early 2005, a meeting of the Homeland Security Advisory Council issued a preliminary conclusion that "each state should establish an information center that serves as a 24/7 'all source,' multi-disciplinary, information fusion center."[6] When the guidelines were released later that year, they fostered a second wave of development. Building on the more general 2003 National Criminal Intelligence Sharing Plan (revised in 2005), the publication specified goals, defined processes, listed components, and included model documents for establishing fusion centers. The National Governors Association, which meets annually and develops "best practices," began discussing centers, eventually including them on the list of recommendations for new governors.

Although the 2005 guidelines provided a blueprint, they were not technically legal authorization. Only in 2007 did the *Implementing Recommendations of the 9/11 Commission Act* provide a legislative mandate for fusion centers, in a section on "Homeland Security Information Sharing Partnerships."[7] The 2007 initiative thus formally included fusion centers in the Information Sharing Environment. The functional standards for the ISE, as discussed in the last chapter, included a list of behaviors that, if done "suspiciously," police should consider as possible pre-terrorism indicators. Reports documenting these behaviors are supposed to be vetted and added to national databases. The information is parlayed into different types of intelligence. With the dots collected, human and computer analysis is applied to connect them. The goal is to identify patterns, which will point to incipient plots or suspicious people. The fusion centers, as sites of information collection and dissemination for federal, state, local and tribal government, are intermediate nodes in this decentralized, jurisdictional web.

What this chapter will explore is how the fusion centers and the data-analysis work done at them figure into a formulation of intelligence as a paradigmatic technology of security, which, in tandem other technologies, presents a distinctive apparatus for dealing with contemporary threats. Foucault, in his 1978-79 lectures, elaborated a conceptualization of security in relation to law and discipline. Each of the three—law, discipline and security—can be understood as a technology that developed and was adjusted to solve problems at a given time. That is to say, Foucault uses them as analytical constructs that refer to and aggregate ways of taking up problems. They can be characterized by their techniques for dealing with features such as space, the uncertain, and norms, with a distinctive logic, mode of action and metric for truth. "Law," as Foucault formulates it, works through a legal/illegal binary. It decrees what *cannot* be done within

[5] "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World. Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal, and Federal Level. Law Enforcement Intelligence Component."
[6] Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 19.
[7] *To Provide for the Implementation of the Recommendations of the National Commission on Terrorist Attacks Upon the United States*, 1st Session, H.R.1 Public Law No: 110-53.

the borders of a territory.[8] The United States passed laws criminalizing every stage of a terrorist act – funding, planning, providing logistical support and carrying it out. The United Nations Security Council (pushed by the US) similarly moved to criminalize these acts globally, by mandating each country to pass equivalent legislation within its territory. "Discipline" functions often in concert, by commanding what *must* be done, tending towards ever more detailed specification, and focusing on the individual body. Shoes are to be taken off to go through airport checkpoints, foreign visitors need the correct visa and can stay an exact amount of time.

"Security," in this schema, is a way of dealing with problems, which deploys law and discipline according to different regulatory norms. Rather than ordering the world into legal and illegal, or dictating behaviors, security uses both strategies to modulate the milieu. "The apparatus of security," Foucault observed, "lets things happen."[9]

> Not that everything is left alone, but *laisser-faire* is indispensable at a certain level… In other words, discipline does not deal with detail in the same way as apparatuses of security. The basic function of discipline is to prevent everything, even and above all the detail. The function of security is to rely on details that are not valued as good or evil in themselves, that are taken to be necessary, inevitable processes, as natural processes in the broad sense, and it relies on these details, which are what they are, but which are not considered to be pertinent in themselves, in order to obtain something that is considered to be pertinent in itself because situated at the level of the population.

Security here is concerned with the distribution and statistical patterning of behavior. Through the collection and study of data on the primary biological life of the population—its birth rates, morbidity and morality statistics, and so forth—the population is constructed as an object. One idea in circulation today is that security requires us to be concerned with not just biological life, but the social life of the population. The term "data-mining" is applied, somewhat unfortunately, to three rather different processes. Data analysis can begin with a person, or with a rule that finds relations between people and behaviors. Or, at its most abstract and controversial, seeks to find patterns of data that will predict future behavior. All three are routinely used as to get intelligence for national security purposes, taking social life as raw data, from family ties and religious affiliations to habits and acts of air travel, online purchasing, social networking and cell phone calls. These, like birth and death rates, are taken to present "natural processes," of normal and abnormal behavior, of legal and criminal lives.

[8] Foucault focuses on the proscriptive rather than the compulsory action of law. Blackstone clearly recognizes both forms of action. "[I]t follows that the primary and principle objects of the laws are RIGHTS and WRONGS. In the prosecution therefore of these Commentaries, I shall follow this simple and obvious distinction; and shall, in the first place, consider the *rights* that are commanded, and secondly the *wrongs* that are forbidden, by the laws of England." Legislation often functions by defining rights and mandating, rather than prohibiting, acts. For Foucault's purposes however, both present the creation of a binary: legal and illegal. William Blackstone, *Commentaries on the Laws of England*, 2nd American ed., 4 vols., vol. I, Book I, Early American Imprints, Series 1, No. 35211 (Filmed) (Boston: American Antiquarian Society and NewsBank, inc, 1766, reprint 1799), 124. Capitalization and italicization in the original.

[9] Michel Foucault, *Security, Territory, Population: Lectures at the Collège De France 1977-78* ed. Michel Senellart, François Ewald, and Alessandro Fontana, trans. Graham Burchell (New York: Basingstoke ; Palgrave Macmillan, 2007), 68.

Nikolas Luhmann marks a distinction between danger and risk. A danger is something that could cause future harm over which one has no control. If, however, control can be levied—a decision made, preparations taken, insurance bought—then the danger is transformed into a risk. The arc of approaches in the contemporary has been to increasingly transform unapproachable dangers (by definition) into something that instead provides purchase. Risks are calculated in relation to a “threat.” Venues such as fusion centers explicitly counter threats. Procedures and technical strategies are developed to turn law, discipline and security into real-world practices. The analysis of information so that it is transformed into intelligence is one such technical strategy. The range of “experts” in this arena includes computer scientists, lawyers, politicians, and intelligence, defense and law enforcement professionals. Fusion centers, data mining, and the issues associated with both, will be discussed below in order.

Fusion Centers

When the law that implemented the 9/11 Commission recommendations, including the fusion center initiative, passed in 2007, I was in the middle of an internship undertaken as part of my doctoral work. The center where I was an intern is located in a grey government building, rising over a dirty and indifferent neighborhood. Guards just inside the entrance direct visitors through a metal detector, and operate a screening belt for bags. Employees with proper identification are waved through to the side. The first time I went, the guards reminded me to remove my shoes and made me leave my cell phone. Back then, in an exertion of control pointless except for its disciplinary effect, phones with cameras were not allowed, and were held at the entrance until the visitor returned. Past the guards, the stone floor stretched out to rows of elevators, each serving a limited block of floors. The elevator corridors are identical except for signs hung high, with tiny numbers identifying the destination. Picking the right row felt uncomfortably like a candid-camera set up. The men on the elevator—there were more men than women—were feds or narcs. The feds were clean-shaven, clean-cut and a bit stiff. They wore suits, and most were FBI. Some of the narcs were actually federal as well, from the DEA, but they are known as the cowboys, the least orthodox of the law enforcement agencies. Others were from regional narcotics operations. They ranged from massive, muscled drug warriors to scruffy uncover officers. There were some women: agents identifiable by their physical fitness, as well as administrators, intelligence analysts, and secretaries.

Once up the elevators, there was a buzzer for the nondescript door of the authorized access area. In fact, this door and those on the same floor that led to DEA intelligence, were so nondescript that even after months working there, I sometimes walked right by them. Fusion centers tend to be imagined as futuristic assemblages with screens up to the ceiling that allow real-time event tracking, and some are, but as the Deputy Director of Intelligence for the Department of Homeland Security in the Bush Administration said, "If you've seen one fusion center—you've seen one fusion center."[10] Mine had cubicles and cheap carpet. Instead, the technology was in the range and depth of access to advanced analysis programs, databases and the equipment available on loan for surveillance operations within the jurisdiction. The office, under a single director, contained a High Intensity Drug Trafficking Area program (HIDTA), and a Regional

[10] Hylton, "Fusion Centers: Giving Cops Too Much Information?."

Terrorist Threat Assessment Center (RTTAC). HIDTAs served as models for many states establishing fusion centers after 9/11, although not everywhere did that result in co-location. In this case, the two organizations worked side-by-side for several years. Each independently received grants and funding, but they shared costs on rent, software purchases and other items. Then the relationship was formalized by combining them into a Regional Intelligence Center. In follow-up interviews two years later, analysts said that the structure and division of work remained much the same, with dual missions sharing space and resources.

The doors opened with RFID-controlled card passes, in addition to the buzzer. All nonemployees had to be met and signed into the visitor's log. The entry way led to a line of cubicles and tall windows over downtown. To the left and right of the workspaces were whiteboards where analysts were supposed to write their Blackberry contact number, regular schedule, and upcoming absences for trainings, meetings or personal reasons. Most employees had long commutes, and used flex-time to work a ten-hour but four-day week, reducing the time and expense of travel. I worked at the end of this row, which did counternarcotics, and opened onto the central room with a meeting and lunch table, and some of the counterterrorism group's desks. We occasionally stood at the windows and watched the cars and panhandlers below with binoculars, looking for crimes and guessing where the frequent, shrill emergency vehicles were headed. Working on crime produced a cheery fatalism. Successes were case-bound, mild corrections to an environment permeated with depravity. "Do the lions ever wipe out the wildebeest?" one DEA agent asked me and then answered immediately. "No, we always catch the weak and sick and stupid. We never get the big bull. In some ways we keep them stronger. The whole point is just to hold the line, to keep the ecosystem in balance." On top of that, bureaucracy could consume hours, even weeks. Frustration with the protection granted to "bad guys," by what were considered absurdly liberal laws and politicians, led my colleagues to joke, "It's good the windows don't open," so that they didn't jump.

"Federal Fusion Center" is something of a misnomer; the median level of federal funding for the centers that existed in 2007 was 21 percent,[11] meaning most of the start-up and operational costs came from redirecting state and local funding streams. Annual budgets at the last estimate ranged from tens of thousands of dollars to several million dollars, with one outlier at reportedly $15 million. Some staff positions are paid out of these budgets; others, however, are often "on loan," seconded from city, state and federal agencies that partly or wholly paid their salaries. For example, where I interned about half of the analysts were seconded from the National Guard. This is also an example of how "information sharing" was adapted into practice at least partially by "people sharing". Army and Air Force National Guard made up the bulk of the HIDTA analysts, and the center also had representatives from sheriff's departments, city police, and the Coast Guard. During the time of my internship, other public service entities were beginning to contribute seconded staff, towards the goal of developing a regional all-hazards center. Functionally, theses seconded individuals were points of contact with their home agency. This helped form the ever-extolled personal relationships of trust. "These things only work when you know someone," was a typical remark, in this case from a drug intelligence analyst named Pete. Such relationships are deemed crucial in intelligence and law enforcement, as already discussed, and also in emergency response, which was part of the fusion center's

[11] Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 33. More recent statistics on fusion centers were not available at the time of writing and the Department of Homeland Security did not respond to inquiries, although they did update the information on their website regarding the number of fusion centers.

regional coordination mission. Gabe, an analyst who was Air National Guard, explained to me how and why his employment arrangement had been worked out.

> Across the board, the occurrence of late, is that it is mandated that the agencies are now going to be cooperative. In DOJ and DOD, information sharing has become the norm. One of the ways that they decided to satisfy this requirement was with agencies like the HIDTA. They figured "we can utilize the National Guard assets to better serve law enforcement." That way they can point to cooperation—we're it. Take communication: if there are National Guard in a location, they can install SiprNet—the military's secure internet protocol router network—and then we, who are here, can use it and be the conduit for sharing the information. That could be necessary in an emergency, and we would be the only ones with access. Or for other kinds of information. One of the things they found along the way, from our military presence in other countries that have narcotics trafficking, is there is always information to be shared in that way. They are always concerned with political correctness though. Because of Posse Comitatus, they needed to make sure they followed guidelines if we were going to provide assistance and support.

Posse Comitatus means "power of the country," and first appeared as an English anti-riot law, in reference to the men of a region who could be called to service. In the aftermath of the US Civil War, the army occupied former Confederate states, to implement Reconstruction policies, and quash any flare-ups of rebellion. After a disputed presidential election, in which the troops were accused of having altered the outcome by their presence at the polls, a congressional deal removed the army from the south. The Posse Comitatus Act of 1878 was then formulated by Southern congressmen intent on preventing renewed federal dominance. The Act's prohibition reinforced that it is foremost a state responsibility to police the land, maintain law and peace, and provide for orderly voting in elections (or to neglect this responsibility, as in the case of access to voting for African-Americans in the former Confederate states when the military withdrew). Posse Comitatus prohibited the army from being used as a domestic police force by the executive branch, and also came to be understood as a powerful restriction on military involvement in domestic affairs. Opponents of fusion centers, and more generally the militarization of government, have raised objections to the National Guards' presence in its name.[12]

The original text of the Act threatened a fine or imprisonment if the military (which at that time was the Army) was used "for the purpose of executing the laws." Federal courts decided that "executing" disallowed an *active* role, such as making an arrest. However, a passive role such as providing "supplies, equipment, training, facilities, and certain types of intelligence information" could be justified,[13] because the military had unique advantages in these arenas. As the task of national security diversified to encompass threats such as drug trafficking and illegal border crossings, "executing the laws" was more and more narrowly defined by judicial interpretation and legislation. Authorized uses of the military increasingly expanded. Weakening of the Act accelerated in the 1980s under President Reagan, who directed the Department of Defense to support counternarcotics and operations against illegal immigrants. Legislation legitimated this kind of military participation as logistical support to civilian law enforcement, not direct

[12] Editorial, "The Military Is Not the Police," New York Times, 30 July 2009.
[13] Craig T. Trebilcock, "The Myth of Posse Comitatus," *Journal of Homeland Security* October(2000).

execution of the laws. The use of soldiers, marines, and National Guard in the 1992 Los Angeles Riots, when the US hosted the Olympics, and on border patrol, followed.

The National Guard analysts often had security clearances and previous intelligence training. They were part of the HIDTA side of the center, and therefore worked on law enforcement narcotics cases, rather than terrorism. Developing a prosecutable case was what was important to the agents for whom the analysts worked. Teams therefore erred on the side of caution when deciding what tasks an analyst seconded from the National Guard could do for a given case, because the distinction between "active" and "passive" could be critical when the case went to court. Gabe described the situation.

> The National Guard provided me with a course that was "Intro to Intelligence and Analytical Concepts." Then I came here [to the HIDTA] and they gave me Penlink [software] training, DEA mobile fleet, more fundamentals. But we don't do work that might enter into the chain of evidence. If it could require court testimony, such as listening on a wiretap, then it is just better that we don't do it. Otherwise we [because we are members of the national guard] might get the case tossed out.

The fusion center was not exactly, or at least literally, a law "enforcement" agency, for either narcotics or terrorism. It was an intermediate node in the Information Sharing Environment, and provided support to and coordination between local, state, tribal and federal agencies for their enforcement activities. Local departments borrowed analysts from the fusion center, which meant they could have help with a case at no cost, while retaining lead agency status and hence the eventual arrest statistics for the investigation. At least, for drug cases they often retained the case, while for terrorism this was rare, and more likely to be temporary. While "enforcement" capabilities in counternarcotics exist across the spectrum, from the federal Drug Enforcement Administration to city police departments, a terrorism-related investigation generally would be passed along to the FBI's Joint Terrorism Task Forces (JTTFs), directly or via the center. A JTTF could be co-located with a fusion center, bringing the center much closer to on-the-ground investigations, although this was not the case where I did research. The joint terrorism task forces included state and local representatives, so that ideally a connection was maintained to the original reporting and jurisdiction of the incident. It became FBI policy after 9/11 that all terrorism tips had be evaluated, but many are not deemed credible enough for further investigation, and are handed back over to the reporting department for non-terrorism related archiving or follow up.

At the local level, dedicated terrorism units and investigations are not common, and commanders tend to be loath to let their subordinates spend time chasing leads instead of dealing with pressing public order and crime issues. They would rather give such investigations to the FBI, although there is a bottom-up tendency to expand the definition of terrorism in order to tap dedicated funding streams favoring counterterrorism, and a convergent top-down tendency in order to justify that allocation. Yet as the instrumentality of this expanding definition indicates, terrorism is not widely viewed as a pressing local issue.[14] Smaller, local departments rank terrorism low in their threat assessments, although concern increases with the size and population density of jurisdictions. The FBI, in contrast, has expertise, equipment, and a clear counterterrorism mission directive covering both intelligence-gathering and investigation.

[14] K. Jack Riley et al., "State and Local Intelligence in the War on Terrorism," in *RAND Infrastructure, Safety, Environment* (2005).

The HIDTA half of the fusion center offered its counternarcotics trainings, specialized tools (surveillance equipment, a wire room) and analyst services to the counties in its region. Support was limited to cases with a drug nexus. The "Terrorism Threat Assessment" half focused, at least in the early days when I was interning, on setting up a communication system. They needed to connect to the federal network in one direction, and to the public and regional first responders in the other direction. "We're trying to make sure that people can do their job," said deputy director Jerome, "which to me is the collection of information from outside resources and developing that information to a point where you have some intelligible intelligence product to give back to them." The other deputy director, Frank, gave me some examples of the system working.

> It might be something as simple as a cop getting a phone call or shopping in a store, or doing a shoplifting case where the people in the store say, "You know, this is going to sound real goofy but we've had a guy come into here for the last two years about every five months and get passport pictures. I think he's a terrorist." Nobody gets a passport that many times. And a little bit of checking finds that over the past two years, four times he's reported a lost passport
>
> Or, a first responder may come to us [at the fusion center] and say, "I got some information on the call that we worked and I just can't tell if there's any truth to this. I need you to process this further. Can you assist? They are reporting to us that their neighbors are terrorists, and all we can determine from our preliminary review is that their neighbors are foreign nationals. We've identified names and identities but we can't identify anything further.

"Do people really call in with that kind of tip?" I asked him. "Absolutely, all the time," he answered. Part of their challenge, though, was just getting word out about what they offered. Like the "Terrorism Liaison Officer" program, which had trouble getting cops to know whom to tell if they had an incident, the HIDTA had to work to make sure local departments knew they were there. "I know you don't like the word 'shop,'" the other analyst, Pete said, "but that is what we do. We have to shop our services to local law enforcement. They don't know what we do until they've worked with us, so we have to go drum up business."

A study in California posed the question, is there "sufficient purely counterterrorist activity to consistently support a fully staffed fusion center"?[15] Of the five center directors queried, "Two responded yes, one responded no, the fourth replied that fusion centers should be all crimes, and one skipped the question." The directors felt that their centers needed to reflect local law enforcement problems. At the Department of Homeland Security and for others who see fusion centers as a solution, the issue of "buy-in," or how to get state, local and tribal law enforcement to actively participate in and support the centers and its information network, is critically important. Homicide, and for that matter, hurricanes and fires, come along much more frequently than terrorist events. Frank pointed out that law enforcement wanted information that was relevant and would let them do a better job.

> When I started at this regional center, I went out and informally interviewed a network of people that I knew, predominantly in law enforcement but across

[15] Nenneman, "An Examination of State and Local Fusion Centers and Data Collection Methods ", 27.

> multiple counties, multiple jurisdictions, and the biggest single thing that I was told was, "Give me something that's pertinent to me locally." If I want to know what's going on in Baghdad, I'll turn on CNN. Most local law enforcement folks seem to be suffering from information overload. Their inbox is absolutely overflowing. And as a result, some had decided that if it was important, someone would make a point of letting them know and they simply wouldn't even find out if that's really the information. Others try to stay on top of it; some found it confusing.
>
> You know what we'd like to see far as intelligence gathering from cops on the street? What we'd like to see and what we're talking about in the state, is having this established TLO [Terrorism Liaison Officers] program and designated TLOs in each department—terrorism liaison officers, who in reality will become general, all-crimes experts because there is no one terrorism issue that people can say "ah-ha, there is definitely a terrorist."

According to the Congressional Research Service, less than fifteen percent of fusion centers describe themselves as focusing solely on terrorism. A little over forty percent described themselves as all-crime, and a similar percentage as all-hazards.[16] The labels, and what they describe, are for practical purposes still under negotiation. "All" can refer to sources of information, the government entities that are collaborating or the threats handled. From all-hazard's origin as a FEMA term, it appears to have become more proactive, shifting from a term of preparedness to one of anticipation and prevention.

> [T]here are some indications that different fusion centers viewed "all-hazards" as pertaining to either their data streams, agency partners, or the center's role. For some, all-hazards suggests the fusion center is receiving and reviewing streams of incoming information (i.e., intelligence and information) from agencies dealing with all-hazards, to include law enforcement, fire departments, emergency management, public health, etc. To others, all-hazards means that representatives from the aforementioned array of public sectors are represented in the center and/or considered partners to its mission. At some centers, all-hazards denotes the entity's mission and scope—meaning the fusion center is responsible for preventing and help mitigating both man-made events and natural disasters. For others, "all-hazards" indicates both a pre-event prevention role as well as a post-event response, and possibly recovery, role.[17]

What the fusion centers describe as being responsive to their constituents, the ACLU has argued is "mission-creep." Once fusion centers are in place and providing communication channels, they can be used to transmit information not only about suspicious activities, but serious weather or accidents. Not incidentally, expanding the scope of the center and involving representatives from more public service institutions also increases the variety and flow of the raw information for intelligence purposes. Thus the ACLU denounces a trend from counterterrorism to all-crimes to all-hazards as bureaucratic profiteering. The tendency of security, as Foucault pointed out, is to expand and include more elements.

"Arguments against fusion centers," reported the Congressional Research Service "often center around the idea that such centers are essentially pre-emptive law enforcement—that intelligence gathered in the absence of a criminal predicate is

[16] Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress."

[17] Ibid.

unlawfully gathered intelligence."[18] In the post-9/11 haste to set up an apparatus to collect and connect the dots, the question of *if* domestic intelligence should take place was replaced with *how* to do it. US security agencies were given a clear and generative mandate to be proactive in preventing terrorism. Nonetheless, there is no clear conception of or simple guide to the legality of pre-emptive law enforcement. Each of the terms is a construct whose meaning is actively mutating. Is it legal for cops to write down suspicious but not necessarily illegal behavior? (The answer there is "yes".) It is legal to investigate someone who has done something suspicious but not necessarily illegal in order to find proof for further investigation? The collection of some information is legal; for law enforcement, other types of information are protected, barring proof of wrong-doing. Legality depends on who is collecting, for what reason, and what will be done with it afterward.

For years, guidelines for the FBI divided investigations into two types: criminal and national security.[19] For these, there were three levels: threat assessment, preliminary investigation, and full field investigation. Each type, and level, had legal thresholds and investigative tools attached to it. The new guidelines issued in 2008 collapsed the distinction between types and reformulated the levels into: assessments, predicated investigations, and enterprise investigations. Thus there were two major shifts. The first was the elimination of the "wall" between criminal and national security investigative areas, and the "wall" between the FBI personnel who worked in the different areas. Instead, the "level of investigation" determined the available investigative tools, with their varying degrees of intrusiveness. The second was a pronounced shift to "proactive information gathering." The guidelines describe the proactive methods of investigation for assessments—which do not require a supervisor's permission or specific suspicion—as relatively non-intrusive, and they offer a nine-point list. Examples are "obtaining publicly available information, checking government records, and requesting information from members of the public."[20] The FBI does not need to receive specific information or an allegation about possible terrorist activity in order to use these authorized methods. The Guidelines add,

> These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.[21]

With the world "solely" more or less unlimited leeway is granted to investigators, in that protection of the First Amendment activities is eliminated, as long as a reason is given for surveillance and documentation.

FBI guidelines do not of course apply to state or local law enforcement. The closest analog is 28 CFR Part 23.[22] The regulation states, "A project shall collect and

[18] Ibid., 11.

[19] The Guidelines draw their authority from Sections 509,510,533, and 534 of title 28, United States Code and Executive Order 12333, issued by President Ronald Reagan, on United States Intelligence Activities.

[20] "The Attorney General's Guidelines for Domestic Fbi Operations," ed. Department of Justice (Washington, D.C.: Office of the Attorney General, 2008).

[21] Ibid., 13.

[22] "28 Code of Federal Regulations Part 23 (Executive Order 12291) Criminal Intelligence Systems Operating Policies ", ed. Department of Justice (Volume 63, Number 250 Federal Register Online

maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." There are two points of note. One, the "reasonable suspicion" requirement means there must be an link to something criminal or suspicion of something criminal that can be verbally articulated (not a gut feeling). This standard, which dates from 1980, is clearly higher than the new one that the FBI has now given itself. Two, 28 CFR Part 23 technically only applies to multi-jurisdictional organizations that receive federal funds, not a local precinct or sheriff's department. Nonetheless, most law enforcement and specifically the fusion centers use it as a guide. Commercial databases, however, with transaction records on purchases, billing addresses for credit cards and shipping, utility bills pertaining to residences, do not. For law enforcement acting under 28 CFR Part 23, in order to search the commercial databases and then store the information, they need a basis for suspicion with regard to the subject on which they are searching. Law enforcement cannot gather the kind of private data in the commercial databases themselves, but they can search those databases for it. Once received in a search, it can be saved. Thus one issue of finicky detail, which typifies why it is difficult to assess exactly what forms of pre-emptive law enforcement and domestic intelligence are illegal, is that in this technicality, for state, local and tribal law enforcement, some of the restrictions on collecting information are overcome. Although direct collection would be illegal, buying is not. The FBI is aware that this is a loophole requiring some angling to slip through. The Electronic Frontier Foundation conducted an inquiry into the privacy policy of the FBI's Investigative Data Warehouse, the large, mysterious database that Bureau analysts can use to mine for data and assemble into intelligence. They submitted Freedom of Information Act requests, and received the following 2005 internal memo from the FBI's Office of Congressional Affairs.

> We had agreed on the following sentence as a way of avoiding some of the intricacies of data mining policy: "Where permitted by law, and appropriate to an authorized work activity, information gleaned from searching non-FBI databases may be included in FBI systems and, once there, may be accessed by employees conducting searches in furtherance of other authorized activities."
>
> Unfortunately, I couldn't get that to fly, since that was the crux of the Senator's inquiry.[23]

In 1976, standards were developed in response to the history of law enforcement abuses exposed by the Pike and Church Committees. These required, among other things, a criminal predicate for a subject to be entered in a criminal intelligence file. However, this does not apply to all information archives, even for law enforcement organizations working under 28 CFR Part 23. Rather, one of the purposes of other databases is to store non-verified information, or information that does not meet more stringent reasonable suspicious criteria.

> Case management databases, tips and leads files, records management systems, criminal history records, and other nonintelligence databases used and maintained by an agency are not required to comply with 28 CFR Part 23. The reason is twofold. The purpose of case management databases is different from a criminal intelligence database. Case management databases are designed to assist a law

via GPO Access: Federal Register, 1980 (1998)).

[23] "Report on the Investigative Data Warehouse ", ed. Electronic Frontier Foundation (2009).

> enforcement agency in managing its activities and provide factual information on subjects. Second, the information stored in these nonintelligence databases is not based on a determination of reasonable suspicion that a subject (individual or organization) is currently engaged in criminal activity. Much of the information stored in those databases tends to fall into one of two categories: uncorroborated information (such as tips) or fact-based information (such as arrest or criminal history information).[24]

The privacy of some uninvolved and innocent people will be intruded upon in the course of an investigation. The idea behind keeping case management and criminal intelligence databases separate is that it puts limits on this intrusion. One of the problems with data aggregation and fusion is that the process can also knock over protective partitions. This is not a new problem. The Privacy Act of 1974 was a response to concerns over how computerized databases could impact privacy by fusing data from different sources to form a too-complete picture of a person's life. Advances in technology have made interpretation of when and how to apply the law complex, and perhaps easier to circumvent. The act requires that when the government collects and shares information about individuals, it give notice to and get consent from them. The act also gives citizens the right to request and see the information the government has about them. The government must keep "fair information practices" and its databases must conform to standards of accuracy. But there were a number of exceptions to the notification requirement even in the original. Namely, law enforcement was exempt, and there was an easily exploitable "routine use" exception. The FBI Guidelines for example, hold the Bureau entirely exempt.

Another concern with the effects of the centers, and previously of task forces, is that they allow "policy-shopping," where investigative teams use the least restrictive requirements of those participating. I had a long interview in 2008 with the director of the fusion center on these topics.

> It is interesting. I am on a national committee that helped write the fusion center guidelines and the criminal intelligence sharing plan, and the federal government came to us and they said, "we might… what do you think about scrapping 28 CFR part 23?" That regulates how we share information. "Why don't we… Do we really need that? Maybe we should just get rid of that." And as a committee of law enforcement guys, where everybody assumed we would embrace that, "oh yeah, the fewer rules we got, the better," instead we all said, collectively, almost unanimously, "we can't get rid of that rule." That is what gives the public confidence and it is also a rule that gives us a benchmark, gives us something to follow. Then we know our expectation. And if we got rid of it, we could have abuses. I mean, people could go off track. And so it was our recommendation that we not. In fact, what we pointed out to the US Department of Justice, who had asked the question, was 28 CFR part 23 only applies, really, to a narrow group of agencies that receive a specific type of information sharing funding. It really doesn't apply to all law enforcement information sharing systems. It is only law enforcement sharing systems that receive money from specific funding streams, federal funding streams. It doesn't apply to federal agencies, doesn't apply to

[24] "Cfr Part 23," in *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Technical Assistance and Training* ed. Law Enforcement Research and Training (Institute for Intergovernmental Research, 2009). http://www.iir.com/28CFR/FAQ.htm#q1

> agencies that fund their own stuff, it doesn't apply even to agencies that get federal funding outside of that stream. But we pointed out that when you look across the board, most state and local agencies, and most regional information sharing projects, like the RISS systems, were all using 28 CFR part 23, many of them voluntarily, because they thought it was a good safeguard. So DOJ, I mean, they were actually shocked. They thought that we would embrace getting rid of the rules, and we didn't.
>
> *Right, well you could have a backlash.*
>
> That is what we thought, and not only a public backlash, but at the end of the day, most of our guys, you know, want… they want a well-regulated business. A lot of us have been in law enforcement a long time and we have seen what happens when we don't police ourselves, when we don't regulate ourselves, when we don't train our people effectively, we don't have rules and regulations. People get in trouble. As far as public confidence, it's bad. And it hurts people's careers.

The director was a career narcotics officer and had spent a lifetime dealing with the public and colleagues in their times of worst stress, fear and anger. He had illusions about neither civilians nor cops. Unlike some more gung-ho believers in righteousness, he refused the argument that law enforcement's desire to catch bad guys would keep them from committing abuses. *The Weekly Standard*, for example, mocked fears that "Uncle Sam could end up listening to your phone conversations, reading your e-mail and monitoring your shopping trips."[25]

> [I]f defense intelligence analysts lose interest in al Qaeda and develop so strong a fascination with the quotidian affairs of John Q. Public that they are willing to risk their careers to abuse the system, that could happen.

The director, who retained some romanticism about policing, also knew intimately the potential for both petty displays of power and serious violations in law enforcement, especially in the way the connection to the "serve and protect" mission was made more abstract by an intelligence assignment.

> I supported that decision to stick with those guidelines and that fact that we ought to re-review them all the time to make sure that they're sufficient. If they aren't, we ought to increase them. The ACLU and other groups that have a concern on privacy will probably never love the fact that we have intelligence fusion centers, and intelligence sharing guidelines between law enforcement. They are concerned about abuses, but I think at the end of the day, as long as we act prudently, and we always keep an eye on the constitutional issues and what is acceptable in society—kind of what the public expectation is—we can develop systems where we won't get in trouble, where the average member of the public says, "yeah, I can live with that, what they're doing is acceptable."
>
> *How can you counter abuses?*
>
> I think a couple of ways, maybe three ways. First is, you have to develop the protocols, the policies. Somebody's got to define what is acceptable and what is

[25] Heather Mac Donald, "Total Misrepresentation," *Weekly Standard*, 21 January 2003.

> not, and the authority to do what we do. I mean that has got to be defined: where do we get our authority and what is acceptable. Then we have to make sure that everybody is trained, and that everybody is trained on the same sheet of music. So people understand what their authority is and what their responsibilities are and what the restrictions are. And then, we have to hold people accountable. There has to be accountability when we violate laws or policies. When we violate laws, there should be criminal penalties. And when we violate policies, there should be administrative penalties. You know at work, sanctions at work. And we need to continue the training process, because it is easy to kinda forget exactly what the policies are, and it is easy to not stay current with changing policies, which change all the time, because laws change or public expectation changes. So it is a matter of recurrent training, keeping that training current and fresh, and constantly reviewing.

Intelligence Analysis and Data-Mining

> These technologies do not "mine for data"; they "mine for knowledge"—they look through data to find knowledge. Calling this process "data mining" is like calling gold mining "rock mining", because we look through rock to find gold.[26]

Subject-based data mining begins with a person, and proceeds to find out information about him or her. Two facets are, perhaps self-evidently, defining. One, the result will be only as good as the data. The information held in databases must accurately refer to a ground truth: an identity that matches a real person, numbers in the correct field and format. Second, it must be organized so that it is possible to pull together that information. For example, in a database of telephone calls, one must be able to check all the numbers called from a subscriber. *Rule-based* data mining starts instead with a rule, which is then used to search databases. For example, *if* multiple purchases of a new precursor used to process methamphetamine were found in conjunction *with* large financial transactions, *then* additional investigation might be warranted into illegal drug manufacture and trafficking. The rule could be drawn from known associations. Or, the rule could be reasonably developed through subject matter expertise in order to find something emergent. With rule-based searches, as with subject ones, having accurate, searchable, relatable data defines their worth.

Patterns are another way of organizing inquiry. Pattern-based searches can be more complex versions of rule-based searches and as with rules, the pattern can be drawn from past incidents or an expert's best guess about scenarios. For example, a pattern could be developed to go through data looking for some or all of the circumstances for the Oklahoma City bombings. Then, another situation matching those circumstances would indicate that a similar terrorism plot might be in the works. Or, a counterterrorism team might come up with a pattern based on recent attacks in another country. One indispensible element here would be the right body of data in which to look for patterns: if local purchases of materials are tracked but everyone in the region buys materials online and delivery can't be tracked, the fact that the materials really are part of

[26] David Jensen, "Data Mining in Networks, Presentation to the Roundtable on Social and Behavior Sciences and Terrorism of the National Research Council, Division of Behavioral and Social Sciences and Education, Committee on Law and Justice, Slide 10," (2002).

the pattern won't help the investigator. Another indispensible element is a training set, a body of real-world data against which the pattern, once identified, can be tested and adjusted, otherwise the original assumptions that define the pattern are wholly limiting. The Oklahoma City bombings are not sufficient to mark all the ways that a terrorism plot could be developed, so as plots are found they must be added to the training set. (One critique of this kind of data mining is that there are not enough plots to populate the training set.) A design in which the pattern is tested against a set and evaluated is called "supervised learning." The original design is increasingly improved so that it matches real patterns. As well, the match must be verified to be something useful about terrorism, not just an intriguing or random statistical correlation.

All of these techniques are limited to what is already known or can be imagined. In other vocabulary, they are in the realm of the possible. The question is, can this limitation be removed? The attempt to do so inverts the search for terrorist patterns. Instead, normal patterns are identified in large bodies of data, and deviations become significant. This way, one does not have to know what one is looking for. "Normal" can be established as the history of the behavior of an individual, a population or other unit. Previous behavior is as distinctive as a signature. Data-mining that seeks this kind of internal variation is therefore called "signature-based anomaly detection."[27] Or, "normal" can be defined in relation to a category of like kinds, such as all households that share certain demographic characteristics.

Supervised learning requires a training set of terrorist indicators. One of its main problems though is too few cases of terrorism incidents and therefore too few sets of pre-incident indicators for which to watch. Unsupervised learning, as anomaly detection is called, requires masses of data about everyday life. It aims to address the challenge of novelty by transforming data into numbers and according importance to difference, repetition, and change. Notably, limitations have not been removed but displaced by inverting the search from one for unusual patterns to one for deviations from the norm. Instead of a pattern of terrorist behavior, there must be patterns of normal behavior.

Data mining refers, evidently, to very different processes. First I will go over the more traditional practices as analysts at the fusion center described them. Then I will describe "predictive" data-mining and accompanying debate.

Criminal Analysis

"It just takes a lot more people to construct a chart, when all you have are sheets of graph paper and a calculator," Pete, a contracted HIDTA analyst, observed dryly.

> Before there was analytic software like Penlink, to look at linkages, you made this kind of triangle chart, and there are places now that do it that way. When I did the criminal intell program up at State [college], it was mostly with people who were already working professionals, who already had jobs in analysis. When I got my internship here, one woman told me it would be great, 'they have all the toys.' A lot of places, these sheets of graph paper, that's it.

[27] "Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Assessment ", 195.

Pete wanted to be interviewed, and so inadvertently transitioned me from the first, participatory phase of fieldwork, in which I was trained in criminal intelligence with a small group of new analysts, into more active inquiry via interviews. Everyone had been informed that I was studying "them". The appropriate forms were signed and announcements sent out. I stated it when introduced. Nothing in day-to-day office life brought up the fact though, but Pete did not let me slide. "When do you want to do that interview?" he asked after I'd been there two months. I got approval from my supervisor, the assistant director, for us to meet during the regular workday and scheduled it for that afternoon. We sat in his cubicle. Gabe, the National Guard analyst who worked between us, listened in and popped his head over the side every once in a while. After a while, I was interviewing them both. "What was your first case?" I asked Pete. "I don't want to say. I don't want you to write it down, but it went well." He was cautious, of course, correctly so. Specific cases were probably not appropriate for a future book or article in anthropology. Even if fully resolved, they could involve a new or clever investigative technique, or a detail might provide too many clues to a guarded identity. "The majority of our time," noted Gabe, "is spent with intelligence analysis that is case-related. I want to demonstrate what I have found out so that case agents can easily understand it. They are the key players."

> We are taking information that case agents have gathered from investigations, and using it to build a bigger picture of who is involved and to what capacity. We try to predict what capacity that might be, using toll records to identify who a particular subject is talking to, getting address information. If it becomes likely that a subject who came up is involved in the case, we could demonstrate a pattern in call activity, for example. We can tell when it is most likely that the person will be on the phone, or maybe what drug is involved. We can pull photos. The agent can put surveillance on him. We can do trash runs with them. We can make photo lineups of those involved. But then we can investigate even deeper: how much is someone a player in the whole operation, and trace out the operation by linking these people together. The analyst can tell who the people communicating with them are, if they are using email accounts that are encrypted, if they have cells that connect over the net. If an agent is going to go on surveillance, you can layout avenues of approach and where to flee, but they are going to want to do that themselves too. Basically, there are so many different means that can provide information. We are trying to put it together in a way the agents can understand.

"How would you describe the analysis process you go through?" I asked Pete.

> When you are putting together a case, you ask yourself, "What holds together and what doesn't?" You get the name of a phone subscriber, the name and address. Sometimes you look up an address but don't find the person's name. So, it could be a fake address that they've used to register for something. You try to establish if it's a home or business. If it's a restaurant, it may be where he works. Or it could be a fake subscriber name. When you look up a name, you say, "maybe that's the person, maybe it's not." For example, with a phone subscriber, maybe the name is Jonathan Smith. You see two people at the house address. One is Jonathan Samson. Maybe he wanted to use his real first name, but a fake last name, because it is easier to keep track of or he figures it's more likely that mail will get delivered
>
> Then you might look at maps, and see what other people are in the building. Sometimes you have to branch fairly far. You might be looking at someone here,

> but when you run the name, the only person is in, say, San Diego. But maybe if you look harder, it might actually be the San Diego person, who is traveling. The driver's license might come up with traffic ticket information, so that might be evidence that the person is traveling here. Seeking those kinds connections are the ones I really like. That's great. The best part is you're figuring out who is doing what and what is where. You're alternating between gathering and hunting. You run a name out in one of the databases, like Accurint or CLETS, looking at information, and you see connections. You go to the agent with the answer, and you're the analyst. They would never have time to track a person down like that.

Accurint is a commercial database used by law enforcement. It is described as a specialized "locate-and-research tool" by its parent LexisNexis®, a massive information organization and retrieval company well known in legal work, academia, government and business. Autotrack, owned by ChoicePoint, is another. Both companies collect information from a vast number of sources and make them available for a fee that can be per search or a flat monthly rate. Different levels of information may be available. Gabe interjected.

> If you are a real estate agent, the level of information is limited. There is more available to law enforcement, and when we log in, it automatically identifies us has having that level of access.

In a pay-per-file arrangement, a search will come back with a list of names and minimal information, and the investigator has to guess which one, or ones, to buy. In 2008, a comprehensive dossier from Accurint was around $5.50. CLETS, which Pete also mentioned, is the California Law Enforcement Telecommunication System and is not commercial. It provides a direct interface with government databases such as the Department of Motor Vehicles (DMV), the National Law Enforcement Telecommunications System (NLETS), the Federal Bureau of Investigation National Crime Information Center (FBI–NCIC), the Criminal Justice Information System (CJIS), and the Oregon and Nevada law enforcement systems.[28]

CLETS contains criminal histories. For law enforcement, access to and the confidentiality of these combined data sources are taken seriously. The result, in fine bureaucratic tradition, is that certification requires a painfully dull training. The daylong course is less on how to use CLETS than on the regulations for appropriate use. Each request for information, for example, must identify the requester, because users are audited every couple of years to make sure that their requests are related to an investigation, and therefore justified. Generic reasons are inadequate. A specific case number or department of corrections number must be provided. This means that for CLETS an analyst generally cannot do searches in order to begin an investigation. Agents and analysts are cautioned not to add just a name to their own searches for a pleading colleague, or to misuse case numbers, for searches that aren't actually unconnected to the case.

> Every database system requires you to justify your search. The DMV for example has a byline for a case number. Each one has an audit trail system. You can't even search your own information without a justifying purpose and it must be law

[28] "Training Bulletin : Automated Information Systems V-C.2 Calea Ref No. 81.2.9, 82.3.6, 82.3.8," (Oakland Police Department, 2000).

> enforcement related.

There are strict rules against looking up people for personal interest or malice—ex-lovers, famous people, the license plate of the person who always takes the best parking spot. These rules are inevitably if seldom broken. Scandal results and controls may be tightened, although the point is that the audit system actually worked to catch the transgressor.

The interminable certification exam for CLETS is available online. It is open-book, and learning, or even memorization, is thereby implicitly downplayed. The point, as Foucault noted, is discipline, careful prescription of how things must be done. "Do you have to be re-certified?" I asked. Gabe answered.

> Not for Accurint and Autotrack, because they are commercial databases, they solely bill us on the searches that we do, but it does have a field for indicating purpose. CLETS on an annual basis will complete an audit, and there is an End User Agreement for every year I will be using. If you have access to the system but haven't been using, it will lock you out. It's a way of controlling who has access. CLETS will remind you if you log in, but otherwise you have to contact a CLETS administrator. Each database is tied to a certain agency, same for WSIN [Western States Information Network], EPIC [El Paso Intelligence Center], DMV.

An agent or analyst begins collecting information on an individual with a search on these or similar databases. Gabe gave a concrete example, starting with a commercial database.

> We're running up someone, and Accurint or Autorack will get us a current telephone number—because the individual called in to order a pizza. The databases we use draw on a lot of open-source information. Most of it is purchasing information, anything from a baby shower registry to having a magazine subscription. Companies will now put forth an option allowing you to opt out, but basically if you buy something, you are giving up privacy. Accurint works better if you give it more specific information. Like, if you put in a Chuck Jones query, you get an astounding number of results. Accurint, rather than attempting to provide this, will not complete the query. It will require that you add something else. Autotrack will give you back a lot, just an endless list. At least with Accurint, it tells you where it got the information. That is really useful.

A commercial database search usually results in several similar appellations, which may be aliases, or pertain to different persons. Addresses can sometimes help sort these names into categories of mere variation versus distinct individuals, because the lack of shared geographic locations or life history at least suggest that the match is coincidental. But relatives, who are not automatically suspected, may reasonably have similar names and have lived together. Making a positive match with the known data can be tricky, and so the first sweep of the net is generally wider, and takes in people who are eventually found to be unconnected. Often it is only possible to narrow the options down to three or four from the limited information given in the initial search, all of which must purchased in order to dig deeper.

Evidently, subject-based analysis blends into a search for links in order to develop criminal intelligence. Hunting leads almost inevitably to gathering and linking, then back to subject specific hunting again. From an inquiry into a given subject, relationships to other people, locations, and activities appear. Pete explained how relationships were identified.

> Say we have an informant and he calls at a specific time asking for some dope. He talks to a subject, and requests it. The guy would call his source. We would be interested in whomever that person called immediately after. For the most cases we are just trying to identify subjects with the toll records, and identify if those persons are also involved in the criminal activity. If they dirty up the phone, we can follow that on a pen register. Another instance would be, a subject who has been arrested, or whose phone has been seized and brought into evidence, we can get numbers off the phone.

Tolls records are lists of the calls made from a number by date and time, obtained from a telecommunications company by administrative subpoena. Hundreds of toll records, many useless, might be collected in order to try to diagram a communication network. Under the Federal Wiretap Act that applies to criminal investigations (called Title III, adopted in 1968 and expanded in 1986), a pen register or “tap and trace” can be requested. This collects call information in real time, useful only for a telephone number confirmed significant to an investigation. Otherwise, it is simply a lot of work. A pen register does not include the content of the communication, unlike a wiretap, which is by several orders of magnitude even more labor intensive and under Title III requires a higher level of authorization (usually a judge’s order). Instead of Title III, the Foreign Intelligence Surveillance Act of 1978, or FISA, applies for national security related surveillance.

As Pete explained, a subject may become a focus of investigation a number of ways. His or her name may be provided by an informant. Someone whose telephone records were subpoenaed might have made calls in a suspicious pattern to the subject’s phone, or the number might have been in a confiscated phone. License plates on a car parked at a house under surveillance could have been traced back to the person. Of course, homes, cars, even houses can be in someone else’s name. These are not proof of wrongdoing, and so they are also ways that information on innocent individuals can get added to a database.

> An investigator, for example, might start the process of developing a criminal case using the information contained in a tips and leads file. Investigating the tips and leads information could produce adequate information that, when analyzed, meets the reasonable suspicion standard. If it meets the reasonable suspicion standard, a record on that subject could be entered into a criminal intelligence database. The information from the tips and leads file, as well as any other investigative information gathered, should be kept as supporting documentation for that record.[29]

The names of individuals not reasonably suspected of criminal involvement can be included in criminal databases, but must carry a clear disclaimer, and be connected to someone who does meet a standard of reasonable suspicion. Records can be kept for the federally regulated time of five years in case the individual surfaces again, but if not, must be permanently erased. This purging is required under 28 CFR Part 23, and therefore considered standard practice. Several different software programs combine analytical

[29] "Cfr Part 23."; "28 Code of Federal Regulations Part 23 (Executive Order 12291) Criminal Intelligence Systems Operating Policies ". http://www.iir.com/28CFR/FAQ.htm

features with databases, and many have built-in deletion features. Records that have been inactive will automatically come up for reevaluation, and erasure.

Thus far the description of data-analysis has been limited to the production of intelligence that is one, criminal, and two, tactical or operational in nature. Criminal information can also be brought together to produce strategic intelligence. “Strategic intelligence analysis,” explained Gabe, “demonstrates patterns.”

> I have done some of it in the past. We were trying to put together a project with an interactive map, showing the locations of gang activity in the areas they claimed. The point was that it could be used by law enforcement to track if the gangs were trying to move into other territories, or to map outbreaks in violence and figure out why it was happening.

The patterns he mentions are statistical representations, rather than the algorithmic abstractions of pure predictive data mining. Several different models have been developed for directing law enforcement resources that rely on calculations of crime trends in different districts and patrol regions. The best known of these is Compstat, a management model credited with New York City’s improved crime rate in the 1990s. Using GIS technology and software databases, “comparative statistics” on crime are mapped in close to real-time. The numbers generated by precinct are used to decide where and when to deploy police officers. The situation is adjusted to prepare for what is expected to happen based on these trends. Any confidence interval is in essence a probability calculation. Intelligence-led policing (ILP) is another managerial model, mentioned in the last chapter. Instead of focusing on middle management’s crime statistics, it began by using data to identify serious recidivist offenders as crime vectors.

> When originally proposed in the early 1990s, intelligence-led policing was seen as a conceptual model that used crime analysis and criminal intelligence in a strategic manner to determine offenders for targeting. Crime reduction tactics would concentrate on enforcement and the prevention of offender activity with a particular interest in using crime intelligence against the activities of prolific and serious offenders. The techniques to be deployed included an expanded use of confidential informants, analysis of recorded crime and calls for service, surveillance of suspects and offender interviews. Where intelligence-led policing was revolutionary was in the use of intelligence derived from covert information as a strategic planning resource rather than as a means to develop case-specific evidence, as had traditionally been the case. Furthermore, intelligence-led policing became synonymous with the greater integration of criminal intelligence and crime analysis.[30]

ILP is rapidly matching Compstat in reputation and use. The model’s focus on “dangerous individuals” lends itself to terrorists as well. But more generally, its emphasis on the collection of information (which could be done through suspicious activity reports) to produce strategic intelligence makes it handily adaptable to a second use in the information-sharing environment.

The collection of data and strategic planning that characterize Compstat and intelligence-led policing had not spread uniformly among departments from which I interviewed people, or the United States more generally. Where it has been adopted,

[30] Ratcliffe, "Intelligence-Led Policing," 268.

empirical inquiry is still needed to ascertain what true change this has meant within precinct walls or on the street. Clearly though, the way it produces information that can be woven into the wider security set facilitates law enforcement's integration into homeland security. Jerome explained how intelligence-led policing fit into the center's work.

> It's the idea that we can use information and develop it though the intelligence cycle and create a product showing trends, projected analyses, future events, or future trends, which is a major thing. We collect the information from pre-incident indicators, things that we know are indicators of a terrorist cycle. As of a week ago, we really didn't have anybody on a state basis looking at pre-incident indicators. And now that they have, last week they called me up and go, "you won't believe this but we just found 4 suspicious incidents that appear to be linked."

Predictive Data Mining

In an interview in 2004, then-Massachusetts Governor Mitt Romney declared.

> Fundamentally, we recognize that we can't protect the homeland by just putting a cop out on the corner of the street. We have too many bridges, roadways, hospitals, schools, tunnels, trains. You just can't protect all of the possible terrorist targets. *You have to find the bad guys before they carry out their bad acts*. That requires intelligence. And the states and localities are going to finally have to be a major part of that.[31]

Predictive data mining is intended to relieve a specific bind. Preventative counterterrorism, or crime for that matter, tends to be referenced in public debate to the Steven Spielberg's 2002 film *Minority Report*, in which psychics could see crimes before they occurred, and people were apprehended on the basis of pre-crime accusations. The allegorical connection between science fiction and reality is the fear that data mining denies the right to prove one's innocence. As was pointedly demonstrated in 2006 when an AOL team released individual search data without names, but journalists and many others managed to correctly identify and contact the actual people who had done the searches,[32] data mining can combine enough sources to identify individual people without the need for personal information such as names. If digital searches are equated with physical searches, and these are conducted on masses of undifferentiated data, there clearly cannot be the particularized reasonable suspicion necessary for the searches that the data mining itself is held to constitute. The mere search constitutes, at an extreme, not only a violation of privacy, but an unwarranted act of suspicion.

Subject searches in law enforcement have traditionally required a predicate, a justification for intruding into someone's life. This protection is based on the Fourth Amendment right to be secure against unreasonable search and seizure. Yet the dream of pattern-based searches is to identify subjects that merit such intrusion before there is a predicate as traditionally understood, and long before they commit an act of terrorism.

[31] Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 17. Italicization added

[32] Michael Barbaro and Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749," *New York Times*, 9 August 2006.

Since the First Amendment protects freedom of religion, speech, the press, to assemble and petition the government, these cannot form the sole basis of suspicion either. Including them in a mass of other information is technically legal although politically delicate. How then does one identify the dangerous individuals?

There remains a genuine divide among experts as to the utility of predictive, pattern-based searches for identifying people who merit further investigation. There is no evidence that this kind of analysis is more effective than others, or that with improvements in technology it necessarily will be. The alternative is standard analytical procedures, in conjunction with human intelligence networks. The question is not posed as either/or, however, but both. All the kinds of data mining involve databases with a lot of personal information in them. By and large, these databases already exist, but they are not already linked, either physically or by an equivalent search. Linking them reduces privacy. On one side, in as much as the data is already held somewhere, not allowing it to be brought together or easily searched is essentially protective inefficiency. Yet, the US Supreme Court, in 1989, called this "practical obscurity" and upheld it as a protected safeguard of privacy.[33]

> Granted, in many contexts the fact that information is not freely available is no reason to exempt that information from a statute generally requiring its dissemination. But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

Practical obscurity is the antithesis of "a seamless network of information sharing" or "connecting the dots." It became an untenable protection for privacy as the narrative of 9/11 placed blame precisely, if not explicitly, on the anonymity of inefficient surveillance and archiving.

Yet the generalized license for intrusion potentially supplied by large-scale data mining is critiqued in an article co-authored by a chief scientist at IBM and the Cato Institute's Director of Information Policy Studies:

> Without patterns to use, one fallback for terrorism data mining is the idea that any anomaly may provide the basis for investigation of terrorism planning. Given a "typical" American pattern of Internet use, phone calling, doctor visits, purchases, travel, reading, and so on, perhaps all outliers merit some level of investigation. [34]

This scrutiny, they suggest, would penalize valued American freedom, let alone, idiosyncrasy. It would be necessary to watch "normal" behavior and deviation from the

[33] *United States Department of Justice Et Al. V. Reporters Committee for Freedom of the Press Et Al. 489 US 749*,(1989).and K. A. Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," *Columbia Science and Technology Law Review* V(2003): 59; *United States Department of Justice Et Al. V. Reporters Committee for Freedom of the Press Et Al. 489 U.S. 749*,(1989).

[34] Jonas, Jeff and Jim Harper. "Effective Counterterrorism and the Limited Role of Predictive Data Mining." December 11, 2006. http://www.cato.org/pub_display.php?pub_id=6784 (accessed January 6, 2009).

norm would be the basis for reasonable suspicion. Privacy for everyone is diminished in this scenario, and at the same time, terrorists could simply act “normally.”

A range of counterarguments have been assembled. Privacy does not trump public safety. Privacy is preserved in the very anonymity of computer abstraction. Better the anonymous analysis of an algorithm than the peering eye of a fellow human. “The search,” one lawyer protested on a technical level, “is not for outliers or deviants from normative models but, rather, for ‘in-liers,’ that is, terrorists engaged in generally normative behaviors but whose links or relationships may reveal illegal organization or activity.”[35] Looking for a pattern of association between unrelated people based on a series of same-actions, such as book purchases, is looking for an association. If two people buy the same book, that might mean they have the same taste in literature and might also buy other books in common. It does not suggest that the people know each other or share other tastes. Instead of *like* behaviors, a counterterrorist search would instead look for unusual relations between people based on *different* kinds of actions, the information on which would be located in dissimilar databases. Department of Homeland Security’s ICEPIC [**I**mmigration and **C**ustoms **E**nforcement **P**attern Analysis and **I**nformation **C**ollection System] program, for example, brings together information from databases on foreign visitors, student and exchange visas, and immigrants, among others, to look for suspicious patterns of relationships.

To protect privacy in advanced data mining, real world “dots” are transformed into numbers. Normal and abnormal flows of data can be described without reference to content. When eddies and ripples are found in these purely numerical flows, content can then be restored so that grounded investigation into what is hopefully (but not at all necessarily) terrorism, stock market fraud or other illegal activities can begin. Instead of using too-rare historical examples of major terrorist events, lower level data are used. The distinction between this and something like Compstat’s representational arithmetic, which might begin with the same law enforcement intelligence in criminal records and commercial data, is that the patterns of the numbers themselves are held to be significant. If they can be modeled and applied to real-world data, they might describe (which would be to predict) what will happen. If there is an identifiable vector in aggregated data, plotters or plots, intervention is possible. Of course, the problem is that patterns in the numbers may mean nothing useful in the real world. As with fractals, another type of pattern explored for predictive use, it is not necessarily useful to turn data into dots and map them.[36] An analyst must check and see what the results mean and if they are pertinent.

The most infamous data-mining project to date is probably the Department of Defense’s Total Information Awareness Program. The goal of what were actually five distinct projects was "to develop technology not only for ‘connecting the dots,’ but also for deciding which dots to connect."[37] With fear of sleeper cells pervading the nation after 9/11, the Pentagon’s Defense Advanced Research Projects Agency (DARPA) sought to

> automatically exact evidence about relationships among people, organizations, places, and things from unstructured textual data...this information can point to the

[35] Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," 63.
[36] Benoit Mandelbrot, Michael Frame, and Nial Neger, "Fractal Geometry," (New Haven, CT: Yale University).
[37] "Report to Congress Regarding the Terrorism Information Awareness Program: Detailed Information," (Department of Defense, 2003), 8.

> discovery of additional relevant relationships and patterns of activity that correspond to potential terrorist events, threats, or planned attacks. These technologies would be employed to provide more accurate, advance warnings of potential terrorist activities by known, or, more importantly, unknown individuals or groups. DARPA believes that they will allow for the identification of connected items of information from multiple sources and databases whose significance is not apparent until the connections are made.[38]

The program would allow “analysts to search vast quantities of data for patterns that suggest terrorist activity.” The Scalable Social Network Analysis project, much like syndromic surveillance in the realm of public health,[39] functioned by defining the significant as relative change in activity. They would “identify the transition of terrorist cells activity from dormant to active state by observing which social network metrics changed significantly and simultaneously."[40]

As the project’s title highlights, public relations were poorly thought-out. John Poindexter of Iran-Contra scandal fame was appointed director. The logo was an eye atop a pyramid, overseeing the planet and the phrase *scientia est potentia* (“knowledge is power”). Drowning in negative media coverage, the project name was changed to Terrorism Information Awareness, a shift from means to ends. Regardless, Congress officially defunded it. By presidential signing statement, though, the programs were renamed and dispersed to other parts of the government.[41] As one critic put it, “The names of key projects were changed, apparently to conceal their identities, but their funding remained intact, often under the same contracts.”[42]

Technical experts are in agreement, however, that “code is law” or “architecture is politics,” the idea that “the architectures of cyberspace are as important as the law in defining and defeating the liberties of the Net.”[43] Programs should be designed so that privacy features are built in. DARPA had claimed that they would ensure "security with privacy," by "providing certain critical data to analysts while controlling access to unauthorized information, enforcing laws and policies through software mechanisms, and ensuring that any misuse of data can be quickly detected and addressed."[44] As a proponent admonished, the net result of complaints was to remove the technological effort from the public sphere where debate could occur.[45]

The issue, one might say, is only partly in the data-mining technology, since in order for any government agency to use even carefully regulated and auditable programs, which DARPA’s Total Information Awareness project promised to develop, massive quantities of data would be have to be collected and housed. Such a database may well exist. The FBI’s Investigative Data Warehouse, or IDW comes close.

[38] Ibid., 7.

[39] Lyle Fearnley, "Detecting the Epidemic: Syndromic Surveillance as Event-Approach Practice," in *Session "Event-Approach Practices" at the American Anthropology Association Annual Meeting* (San Francisco2008).

[40] "Report to Congress Regarding the Terrorism Information Awareness Program: Detailed Information," 9.

[41] Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," 10.

[42] Shane Harris, "Tia Lives On," *National Journal*, 23 February 2006.

[43] Lawrence Lessig, "The Code Is Law," *Industry Standard*(1999).

[44] "Report to Congress Regarding the Terrorism Information Awareness Program: Detailed Information," 6.

[45] Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data."

> As of January 2005, the IDW contained "more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds." A chart in the FBI documents shows IDW growing rapidly, breaking the half-billion mark in 2005. By March 2006, the IDW had 53 data sources and over half a billion (587,186,453) documents. By September 2008, the IDW had grown to nearly one billion (997,368,450) unique documents. The Library of Congress, by way of comparison, has about 138 million (138,313,427) items in its collection. In addition to storing vast quantities of data, the IDW provides a content management and data mining system that is designed to permit a wide range of FBI personnel (investigative, analytical, administrative, and intelligence) to access and analyze aggregated data from over fifty previously separate datasets included in the warehouse. Moving forward, the FBI intends to increase its use of the IDW for "link analysis" (looking for links between suspects and other people—i.e. the Kevin Bacon game) and to start "pattern analysis" (defining a "predictive pattern of behavior" and searching for that pattern in the IDW's datasets before any criminal offence is committed—i.e. pre-crime).[46]

According to a representative of the FBI’s Foreign Terrorist Tracking taskforce, which helped develop the system,

> About a quarter of the information comes from the FBI's records and criminal case files. The rest—including suspicious financial activity reports, no-fly lists, and lost and stolen passport data—comes from the Treasury, State and Homeland Security departments and the Federal Bureau of Prisons… Names, Social Security numbers and driver's license details can be linked and cross-matched across hundreds of millions of records.[47]

"It appears to be the largest collection of personal data ever amassed by the federal government,"[48] noted the senior council of the Electronic Frontier Foundation, a civil liberties watch group focused on the digital realm. What regulations there are on this is difficult to ascertain. In some senses, it is a misleading question. Giant warehouses can be made obsolete by a program that structures queries into different databases, which one of the DARPA programs aimed to develop, and certainly exist in varying degrees of power. Prohibiting consolidated databases would not necessarily inhibit the practices they facilitate.

Pulling together commercial, law enforcement and other data creates a significant alteration of the previous standard of privacy. This would be an issue even if the FBI’s data warehouse were found to be a paragon of efficiency and due privacy controls, and even if counterterrorism data mining required no additional collection of data. Mission-creep here is “the use of data for purposes other than that for which the data was originally collected.”[49] Various proponents of the massive collection of data for counterterrorism purposes have argued that mission-creep can be guarded against, but that having the data available is indispensible. Not utilizing commercial information in nation security efforts, they say, handicaps law enforcement and defense efforts. There

[46] "Report on the Investigative Data Warehouse ", 1-2.

[47] Ellen Nakashima, "Fbi Shows Off Counterterrorism Database," *Washington Post*, 30 August 2006.

[48] Ibid.

[49] Seifert, "Data Mining and Homeland Security: An Overview (Updated)," 27.

are two counterarguments. One, businesses are checked by consumer perception and interest as politicians are checked by constituent goodwill. People vote with their wallets and in elections. Civil and military servants are bound much more loosely than politicians, who must answer to their electors. Government has recourse to secrecy beyond that of corporations, which can serve to mask abuse. Two, businesses aggregate information useful to them in targeting sales, detecting fraud and so forth. This is much more limited than the massive accumulation of data such as that in the FBI's Investigative Data Warehouse. It is not simply a matter of denying the government what businesses already have, but a distinct power that would be solely that of the government, and given the government's control of the criminal justice system, one with considerably greater consequences.

Considerations

Intelligence failure presents a paradox: it is both avoidable and yet inevitable. Any given successful attack could have been avoided if the right steps had been taken. Failure is therefore, strictly speaking, preventable. To take the right steps *always*, however, is an impossible absolute. Failure on a greater temporal scale is unpreventable. No theoretical solution has been found to this dilemma. After Pearl Harbor, this formulation of the problem of intelligence and its limits shaped the simultaneous build-up of intelligence and preparedness strategies. After 9/11, an initial intensification of both juridical and disciplinary measures gave way to intelligence as a technology of security and the ambition to overcome the failure's hex. Instead of micro *control*, there would be micro collection of dots and data, and in their natural flow, the patterns of the future would be revealed and open to intervention.

Law, discipline and security operate with varying degrees of dominance in different realms. The police of course combine law and discipline in many ways, in the fulfillment of their duties and in internal regulation. Intelligence, rather than prohibiting potentially threatening acts, documents and studies them. The mission is data itself; the metric of good or bad refers to more complete information. It takes up and even multiplies juridical and disciplinary elements, then redeploys them to constitute its own object, that of knowledge.[50] Law enforcement is organized in a continuous feedback system that nonetheless accepts, and actually requires, crimes to continue occurring. Technologies that work on the level of individual crimes or cases are meant to minimize the overall level of crime but there is no expectation of eliminating it. "Zero-tolerance" rhetoric is rather in contradiction to police practice. In all practical matters, law enforcement assumes that crime will continue. This fact is the foundation of the "new intelligence architecture." In the accumulation of details, processes will be revealed.

These distinctions between law, discipline and security map onto the differences in criminal and national security intelligence that surface problematically in their junction. Fusion centers fuse not simply different sources of information. They also join strategic rationalities (prevention, preparedness, anticipation/prediction of events); local, state and federal jurisdictional powers; law enforcement with other first responders; military and private sector representatives; and missions ranging from terrorism to all-crimes to all-hazards; as well as geographically specific threats from drug trafficking routes to port harbors. They are venues where law and discipline are brought together in the

[50] Foucault, *Security, Territory, Population: Lectures at the Collège De France 1977-78* 23.

management logic of security, and information is turned into intelligence. Data analysis, in its distinctively different guises, is a key technique.

Increased surveillance and data sharing within the Suspicious Activity Reporting system introduces a new element. There has been some, perhaps surprisingly little, debate about how to best protect privacy yet still use the information already held by commercial and government databases in the work of protecting against terrorism. Increased surveillance, however, from tracking emails and phone calls to behavior on the street, means more information, and more different kinds of information. Should law enforcement be doing intelligence? Are they prepared, by training or experience, to perceive and deal appropriately with non-criminal, but somehow suspicious behavior? Historically, the farther law enforcement has gotten from case-specific work, the more prevalent are violations of civil liberties.[51] Yet, the fact that for most fusion centers, (outside of New York, Los Angeles and Washington, DC) the actual amount of terrorism-related activity is small means that a greater percentage of analysts' time is spent on criminal cases. For these, the law is everything.

Any transgression of criminal justice procedure might appear in court, and years of work by agents and analysts can be thrown out. Agents know the law enforcement rules and are accustomed to following them. Analysts and agents want to keep their cases. If they come from a law rather than intelligence background, and there is a chance for criminal prosecution, they will tend to remain within investigative guidelines. This creates a work environment that suggests that integrating the police into intelligence would have less of a detrimental effect than feared. Of course, from an intelligence perspective, law enforcement's goal of an indictment is what diminishes the advisability of engaging them in such tasks to begin with, because more valuable information may be gained from surveillance rather than arrests.

The proliferation of information, globalization, and catastrophic events has been described as a massive increase in uncertainty. Yet predictive data mining deploys certainty—certainty that events will occur, certainty that a massive event is composed of myriad microevents. If this conceptualization works, no one has to figure out what form the threat will take. It is enough that there be one. Dots are fit into patterns in which the potential for events can be discerned, and the human participants identified. The events remain unformed, or unactualized,[52] and their potential is relocated into the figure of the terrorist, the dangerous individual. One of Foucault's questions was if "we can really speak of a society of security… a general economy of power which has the form [of], or which is at any rate dominated by, the technology of security"?[53] If not all of society—an imprecise concept at any rate—security as a technology operating through modulation, periodic assessment and correction has come to dominate intelligence.

This distinctive approach and manipulation of law and social order can be recognized in the Information Sharing Environment, with its multiple techniques for collecting and connecting data, the development of the fusion centers, and the dream of predictive data mining. At the level of the police officer documenting public behaviors and detaining those who are perceived as suspicious, there is a disciplinary effect on freedom of action, control exerted as to what one can do and how one should behave. A suspicious activity report in relation to the larger information-sharing network, however, is exactly about information that must circulate if it is to be effective. The word seamless,

[51] Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 11.
[52] Deleuze, *The Logic of Sense*
[53] Foucault, *Security, Territory, Population: Lectures at the Collège De France 1977-78* 25.

found throughout government documents, contains a clue. Terrorism was understood as a nation-state problem, and is now one of networks. A network is, as mentioned, not *seamless*. It is composed of links between nodes, a compilation of seams. The seamlessness, or wholeness, is not the idea of a single object, but rather perfect liaison between the elements, of perfect transmission and reception of information.

In this light, security versus freedom is not the right formulation. Freedom rather becomes necessary to security, meaning: we can think of security practices as a combination of techniques and rationalities brought together in a technology. These are characterized by freedom of circulation of information, so that the information can turn into knowledge, and this can in turn produce the related sense of security as a way of dealing with threats. Intelligence cannot function through absolute control. Things must happen. Meetings must take place as tiny pieces of a larger puzzle. Imperfect discipline and minor infractions of the law are tools to coerce the development of an informants-network, or the entry points to tracking more important schemes. They can, and in fact must, occur as part of the milieu, if there is to be data flowing through the information environment.

Yet, consider information sharing as a form of secrecy.[54] The term refers exclusively to sharing within government and even in principle does not imply open government or transparency. To the contrary, that which is freely available does not need to be shared. The Information Sharing Environment is part of a portfolio of government policy that provides knowledge as a solution, ensuring security through the authorized, but not wholly free, flow of information. It seems to obscure a debate about where the information comes from. Information sharing does not per se mean domestic intelligence,[55] but in policy and practice, the two are well on their way to inseparability.

Counterintelligence in the United States was established as a law enforcement matter through a specific sequence of logic, lent credibility by a history of abuses. International law says little about spying beyond permitting satellite or electronic surveillance. Positive law, such as bilateral treaties, and customary law, as accepted by the international community, are silent about human spies. Nations recruit, train, and pay intelligence operatives; their activities are sanctioned abroad. Spy activities are legal against others. Yet they are illegal against citizens, or the self-same government. If domestic intelligence meant spying within the nation, on citizens, it was illegal. Counterintelligence was instead long conceptualized as pertaining to people who were in the US and breaking national laws by spying or plotting for other countries. Reasonably, then, it was a juridical and disciplinary matter, dealt with by investigations into criminal wrongdoing. Yet, law and discipline alone were inadequate to prevent 9/11. Intelligence had to be reconfigured to meet a perceived need.

The issue is not choosing between this system and doing nothing, but rather, what is to be done? Security will tend to expand. The network of knowledge will form a web of security but that web will continue enveloping more elements. It does not have a principle of limitation—one is never too secure. If knowledge is a solution, then more and more knowledge will be needed. Frank offers the last, but not final, word.

Intelligence, this new age of intelligence, is going to come out truthfully through law

[54] Steven Aftergood, "Information Sharing as a Form of Secrecy," in *Secrecy News* (Federation of American Scientists Project on Government Secrecy, 2009).
[55] Timothy R. Sample, "A Federal Approach to Domestic Intelligence," in *Vaults, Mirrors, and Masks : Rediscovering U.S. Counterintelligence*, ed. Jennifer E Sims and Burton L Gerber (Washington, D.C.: Georgetown University Press, 2009), 242.

enforcement as the natural outlet. They're taking intelligence and pushing it because the emphasis is on prevention. And it's simply talked about. It's a collective focus locally, nationally and with other nations. In the past, these were deep dark secrets that were talked about in shadows. I think we have a different perspective now, maybe due to the nature of information, maybe due to the asymmetrical warfare that terrorism brings to us. I'm not really sure what the cause is but I think there should be a big recognition now about the role of intelligence from a daily operational perspective, for all of us.

BIBLIOGRAPHY

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. New York: W.W. Norton, 2004.

"28 Code of Federal Regulations Part 23 (Executive Order 12291) Criminal Intelligence Systems Operating Policies ". edited by Department of Justice, 71752-53. Volume 63, Number 250 Federal Register Online via GPO Access: Federal Register, 1980 (1998).

"About Interpol." INTERPOL.

Adenaes, Johannes. "Deterrence - the Concept. A Historical Perspective, Empirical and Ethical Questions, General Deterrence: Myth or Reality?" In *Law Library Crime and Justice Vol 2*.

Aftergood, Steven. "Information Sharing as a Form of Secrecy." In *Secrecy News*: Federation of American Scientists Project on Government Secrecy, 2009.

Agamben, Giorgio. "Security and Terror." *Theory and Event*,no. 4 (2002).

The Apollon, 22 U.S. (9 Wheat.) 362 362, 366-67, (1824).

Arkes, Hadley. "Strauss on Our Minds." In *Leo Strauss, the Straussians, and the American Regime*, edited by Kenneth L. Deutsch and John A. Murley. New York: Rowman & Littlefield, 1999.

Ashcroft, John. "Fy 2003 Performance & Accountability Report." edited by Department of Justice. Washington, DC: Office of the Attorney General 2004.

"The Attorney General's Guidelines for Domestic Fbi Operations." edited by Department of Justice. Washington, D.C.: Office of the Attorney General, 2008.

Baer, Robert. "When the State Police Fingers Terrorists." *Time Magazine*, 17 October 2008.

Barbaro, Michael, and Tom Zeller Jr. "A Face Is Exposed for AOL Searcher No. 4417749." *New York Times*, 9 August 2006.

Barry, Tom. "The Neocon Philosophy of Intelligence." *Foreign Policy in Focus* (2004).

Baudrillard, Jean. "L'esprit Du Terrorisme " *Harpers*, February 2002.

Beccaria, Cesare. "On Crimes and Punishments." Liberty Library of Constitutional Classics 1819 (1764).

Belenko, Steven R., ed. *Drugs and Drug Policy in America: A Documentary History*. Westport, CT: Greenwood Press, 2000.

Bensa, Alban, and Eric Fassin. "Qu'est-Ce Qu'un Événement? Les Sciences Sociales Face À L'événement." *Terrain, revue d'ethnologie de l'Europe* 6 mars 2002, 5-20.

Bettenhausen, Matthew. "Statement for 'Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs', Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment." Washington, DC: Committee on Homeland Security 2008.

"The Bioterrorism Threat: Strengthening Law Enforcement." INTERPOL.

Black's Law Dictionary. Edited by Bryan A. Garner. 8th ed. St. Paul, MN: Thomson West, 2004.

Blackstone, William. *Commentaries on the Laws of England*. 2nd American ed. 4 vols. Vol. I, Book I, Early American Imprints, Series 1, No. 35211 (Filmed). Boston: American Antiquarian Society and NewsBank, inc, 1766, reprint 1799.

"Book Review of Handbook of Intelligence and Guerrilla Warfare by Alexander Orlov."

Studies in Intelligence 8, no. 8 (1963).

Brent, Roger. "Testimony of Roger Brent, Phd to the U.S. House Homeland Security Committee, Subcommittee on Prevention of Nuclear and Biological Attack ". Washington, DC, 2005

Bruce, James B. "Making Analysis More Reliable: Why Epistemology Matters to Intelligence." In *Analyzing Intelligence: Origins, Obstacles and Innovations*, edited by Roger Z. George and James B. Bruce. Washington, D.C.: Georgetown University Press, 2008.

———. "The Missing Link: The Analyst-Collector Relationship." In *Analyzing Intelligence: Origins, Obstacles and Innovations*, edited by Roger Z. George and James B. Bruce. Washington, D.C.: Georgetown University Press, 2008.

Bush, George W. "Transcript of Governor George W. Bush's Remarks: A Distinctly American Internationalism, December 19th, 1999." FAS, http://www.fas.org/news/usa/1999/11/991119-bush-foreignpolicy.htm.

———. "Transcript of President Commemorates 60th Anniversary of V-J Day, August 30th, 2005." Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2005/08/20050830-1.html

———. "Transcript of President's Remarks on the Uss Enterprise on Pearl Harbor Day: We're Fighting to Win - and Win We Will, 7 December, 2001." Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2001/12/20011207.html.

———. "Transcript of Remarks by the President to Employees at the Pentagon: Guard and Reserves "Define Spirit of America, September 17th, 2001." Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2001/09/20010917-3.html.

———. "Transcript of Remarks by the President, Secretary of State Colin Powell and Attorney General John Ashcroft: President Urges Readiness and Patience, September 15th, 2001." Office of the Press Secretary, http://www.whitehouse.gov/news/releases/2001/09/20010915-4.html

Carus, W. Seth. "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents since 1900." Washington, D.C.: Center for Counterproliferation Research, National Defense University 2001.

Cascio, Jamais. "Legacy Futures." *Open the Future*, 8 December 2008.

"Cfr Part 23." In *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Technical Assistance and Training* edited by Law Enforcement Research and Training: Institute for Intergovernmental Research, 2009.

Chesney, Robert. "Federal Prosecution of Terrorism-Related Offenses: Conviction and Sentencing Data in Light of The "Soft Sentence" And "Data Reliability" Critiques." *Lewis & Clark Law Review* (2007).

Chickering, Roger, Stig Förster, and Bernd Greiner, eds. *A World at Total War: Global Conflict and the Politics of Destruction, 1937–1945*, Publications of the German Historical Institute. Cambridge: Cambridge University Press, 2005.

Clarke, Richard A. *Against All Enemies: Inside America's War on Terror*. New York: Free Press, 2004.

Collier, Stephen J. "Enacting Catastrophe: Preparedness, Insurance, Budgetary Rationalization." *Economy and Society* 37, no. 2 (2008): 224 - 50.

Collier, Stephen J., Paul Rabinow, Christopher Kelty, Lyle Fearnley, Carlo Caduff, Tobias Rees, Colin Koopman, Frederic Keck, Meg Stalcup, and Gaymon Bennett.

"Concept Work: "Vital"." In *Concept Work*, 17 August, 2009.

"Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction." London, Moscow and Washington: United Nations, 1972.

Cooper, Melinda. "Pre-Empting Emergence: The Biological Turn in the War on Terror." *Theory, Culture & Society* 23, no. 4 (2006): 113-35.

Danilenko, G M. *Law-Making in the International Community*. Edited by M. Nijhoff. Vol. 15, Developments in International Law,. Boston: Dordrecht, 1993.

Danzig, Richard. "Proliferation of Biological Weapons into Terrorist Hands." *The Challenge of Proliferation* (2006).

Davis, Jack. "Improving Cia Analytic Performance: Analysts and the Policymaking Process." *Sherman Kent Center for Intelligence Analysis Occasional Papers*,no. 2 (2002), https://www.cia.gov/library/kent-center-occasional-papers/vol1no2.htm.

Dean, Edgar Packard. "Reviewed Work(S): Electoral Procedure under Louis Philippe by Sherman Kent." *The American Historical Review*, October 1938, 112-15

Defoe, Daniel. *A Journal of the Plague Year*, The World's Classics. Oxford New York: Oxford University Press, 1990 (1722).

Deleuze, Gilles. *The Logic of Sense* Translated by Mark Lester and Charles Stivale. New York: Columbia University Press, 1990.

Deutsch, Kenneth L., and John A. Murley, eds. *Leo Strauss, the Straussians, and the American Regime*. Lanham, MD: Rowman & Littlefield Pub., 1999.

Doctorow, Cory. "Fake Dhs "Photography License" For Fake No-Photos Laws." *Boing Boing*, 15 May 2009.

"Doctors: Tb Traveler's Diagnosis More Treatable Than Thought." *CNN*, 4 July 2007.

Donald, Heather Mac. "Total Misrepresentation." *Weekly Standard*, 21 January 2003.

Doyle, Charles. "The USA Patriot Act: A Sketch." Congressional Research Service, 2002.

Drury, S. B. "The Esoteric Philosophy of Leo Strauss." *Political Theory* 13, no. 3 (1985): 315-37.

Editorial. "The Military Is Not the Police." *New York Times*, 30 July 2009.

"Editorial, the Limits of Hindsight." *Wall Street Journal*, 28 July 2003.

Ellis, Jason D. "The Best Defense: Counterproliferation and U.S. National Security." *Washington Quarterly* 26, no. 2 (2003): 115-33.

Falkenrath, Richard A. "The 9/11 Commission Report : A Review Essay " *International Security*,no. 3 Winter 2004/05 (2005).

Fassin, Eric. "Sexual Events: From Clarence Thomas to Monica Lewinsky." *Differences: A Journal of Feminist Cultural Studies*,no. 2 (2002).

Feakes, Daniel. "Global Society and Biological and Chemical Weapons." In *Global Civil Society Yearbook*, edited by Mary Kaldor, Helmut Anheier and Marlies Glasius, 87-117: Oxford University Press, 2003.

Fearnley, Lyle. "Detecting the Epidemic: Syndromic Surveillance as Event-Approach Practice." In *Session "Event-Approach Practices" at the American Anthropology Association Annual Meeting*. San Francisco, 2008.

"Findings and Recommendations of the Suspicious Activity Report (Sar) Support and Implementation Project." Bureau of Justice Assistance, 2008.

Foucault, Michel. "About the Concept of The "Dangerous Individual" In Nineteenth-Century Legal Psychiatry." In *Power: Essential Works of Foucault 1954-1984*, edited by James D. Faubion, 176-200. New York: The New Press, 2000.

———. "The Confession of the Flesh." In *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, edited by Colin Gordon, 194-228. New York: Pantheon Books, 1980.

———. "Polemics, Politics and Problematizations." In *Aesthetics, Method and Epistemology*, edited by James D Faubion. New York: New Press, 1998.

———*. Security, Territory, Population: Lectures at the Collège De France 1977-78* Translated by Graham Burchell. Edited by Michel Senellart, François Ewald and Alessandro Fontana. New York: Basingstoke ; Palgrave Macmillan, 2007.

Friedman, Thomas L. "No Way, No How, Not Here." *New York Times*, 17 February 2009.

"Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World. Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal, and Federal Level. Law Enforcement Intelligence Component." edited by Department of Justice, 2005.

Galison, Peter. "Devise and Dissent: The Patriotic, but Unpopular, Career of J. Robert Oppenheimer." *Slate*, 2005.

Gannon, John C. "Managing Analysis in the Information Age." In *Analyzing Intelligence: Origins, Obstacles and Innovations*, edited by Roger Z. George and James B. Bruce. Washington, D.C.: Georgetown University Press, 2008.

German, Mike, and Jay Stanley. "Fusion Center Update." American Civil Liberties Union, 2008.

Goodman, Allan E., Gregory F. Treverton, and Philip Zelikow. *In from the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence* New York: Brookings Institution Press, 1996.

Graham, Bob, Jim Talent, Graham Allison, Robin Cleveland, Steve Rademaker, Tim Roemer, Wendy Sherman, Henry Sokolski, and Rich Verma. "World at Risk: The Report of the Commission on the Prevention of Wmd Proliferation and Terrorism." New York, 2008.

"Guidance Regarding the Use of Race by Federal Law Enforcement Agencies." U.S. Department of Justice, http://www.usdoj.gov/crt/split/documents/guidance_on_race.php.

Guillemin, Jeanne. *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. New York: Columbia University Press, 2006.

Hallissy, Margaret. *Venemous Woman*. Westport, Conn: Greenwood Press, 1987.

Harmon, Jane. "Statement to the House, Subcommittee on Intelligence, Information Sharing & Terrorism Risk "The Future of Fusion Centers: Potential Promise and Dangers"." Washington, DC: Committee on Homeland Security 2009.

———. "Statement to the House, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs"." Washington, DC: Committee on Homeland Security 2008.

Harris, Rob. "The Enemy Within: Kevin James and the Jis Conspiracy " *Frontline PBS*, 2006.

Harris, Shane. "Tia Lives On." *National Journal*, 23 February 2006.

Hayes, Christopher. "The Good War on Terror: How the Greatest Generation Helped Pave the Road to Baghdad." *In These Times*,no. 8 September (2006), http://www.inthesetimes.com/main/article/2788/.

Hedley, John H. "The Evolution of Intelligence Analysis." In *Analyzing Intelligence: Origina, Obstacles, and Innovations*, edited by James B. Bruce and Roger Z. George, 19-34. Washington, DC: Georgetown University Press, 2008.

Herman, Michael. *Intelligence Power in Peace and War*. Cambridge, England ; New York: Cambridge University Press, 1996.

Hersh, Seymour M. "Selective Intelligence." *The New Yorker* 79, no. 11 (2003): 044.

Honegger, Barbara. " Nps News Profile Nps Prof Publishes Groundbreaking Book on Bioweapons

Monday, November 17, 2008. National Security Affairs Assistant Professor Anne L. Clunan)." *News, Center for Contemporary Conflict, Naval Postgraduate School*, 2008.

Hylton, Hilary. "Fusion Centers: Giving Cops Too Much Information?" *Time Magazine*, 9 March 2009.

"Information Sharing Environment (Ise) Functional Standard (Fs) Suspicious Activity Reporting (Sar) Version 1.5." edited by Program Manager for the Information Sharing Environment (PM-ISE): Office of the Director of National Intelligence, 2009.

"Information Sharing Environment Implementation Plan." Office of the Director of National Intelligence, http://www.ise.gov/pages/vision.html.

Intelligence Reform and Terrorism Prevention Act of 2004. PL 108–458. 108th Congress, 17 December 2004.

Jackson, Brian A., Darcy Noricks, and Benjamin W. Goldsmith. "Current Domestic Intelligence E." In *The Challenge of Domestic Intelligence in a Free Society : A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, edited by Brian A. Jackson, 49-77. Arlington, VA: RAND, 2009.

Jensen, David. "Data Mining in Networks, Presentation to the Roundtable on Social and Behavior Sciences and Terrorism of the National Research Council, Division of Behavioral and Social Sciences and Education, Committee on Law and Justice, Slide 10." 2002.

Johnson, Loch K. *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven: Yale University Press, 1996.

Johnston, Rob. *Analytic Culture in the Us Intelligence Community: An Ethnographic Study*. Washington DC: Central Intelligence Agency, 2005.

Jones, Seth G., and Martin C. Libicki. *How Terrorist Groups End: Lessons for Countering Al Qa'ida*. Santa Monica: RAND Corporation, 2008.

Jules, Lobel. "The Commander in Chief and the Courts." *Presidential Studies Quarterly* 37, no. 1 (2007): 49-65.

Kam, E. *Surprise Attack: The Victim's Perspective*. Cambridge: Harvard University Press. , 1988.

Kam, Ephraim. *Surprise Attack : The Victim's Perspective*. Cambridge: Harvard University Press, 2004.

Katz, Barry M. "The Criticism of Arms: The Frankfort School Goes to War." *Journal of Modern History* 59, no. 3 (1987): 439-78.

———. *Foreign Intelligence : Research and Analysis in the Office of Strategic Services*

1942-1945. Cambridge: Harvard University Press, 1989.

Kean, Thomas. "Interview." *Frontline PBS*, 27 March 2006.

Kennan, George. "The Long Telegram." Moscow: State Department, 1946.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton, N.J.,: Princeton University Press, 1966 (1949).

———. *Strategic Intelligence for American World Policy*. Princeton, N.J.,: Princeton University Press, 1966.

———. *Writing History*. 2d ed. New York: Appleton-Century-Crofts, 1967 (1941).

Kent, Sherman, and Donald Paul Steury. *Sherman Kent and the Board of National Estimates: Collected Essays*. Washington, D.C.: History Staff, Center for the Study of Intelligence Central Intelligence Agency, 1994.

Kent, Sherman, and Sally Newell Thacher. *Reminiscences of a Varied Life: An Autobiography*. Washington, D.C.: E.G. Kent, 1991.

Kilcullen, David. "Ethics, Politics, and Non-State Warfare: A Response to GonzáLez." *Anthropology Today*,no. 3 (2007).

King, Nicholas B. "Dangerous Fragments." *Grey Room* Spring, no. 7 (2002): 72-81.

Kissinger, Henry A. "National Security Study Memorandum 59." Washington D.C.: National Security Council, 1969.

Kittelsen, Sonja. "Conceptualizing Biorisk: Dread Risk and the Threat of Bioterrorism in Europe." *Security Dialogue* 40, no. 1 (2009): 51-71.

Lakoff, Andrew. "The Generic Threat, or How We Became Unprepared." *Cultural Anthropology* 23, no. 3 (2008): 399-428.

Langlitz, Nicolas. "Pharmacovigilance and Post-Black Market Surveillance." *Social Studies of Science* 39, no. 3 (2009): 395-420.

Leitenberg, Milton. *Assessing the Biological Weapons and Bioterrorism Threat*. Carlisle, PA: Strategic Studies Intitute, 2005.

———. "Bioterrorism, Hyped." *Los Angeles Times*, 17 February 2006.

Lessig, Lawrence. "The Code Is Law." *Industry Standard* (1999).

Levitt, Matthew, and Michael Jacobson. "The Money Trail: Finding, Following, and Freezing Terrorist Finances." In *Policy Focus*: Washington Institute for Near East Policy, 2008.

Libicki, Martin C., and David R. Howell. "Privacy and Civil Liberties Protections in a New Domestic Intelligence Agency." In *The Challenge of Domestic Intelligence in a Free Society : A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, edited by Brian A. Jackson. Arlington, VA: RAND, 2009.

Littlewood, Jez. "Managing the Biological Weapons Problem: From the Individual to the International." In *Weapons of Mass Destruction Commission (WMDC) Papers and Studies*, 2004.

Lowenthal, Mark M. "Intelligence in Transition: Analysis after September 11 and Iraq." In *Analyzing Intelligence: Origins, Obstacles and Innovations*, edited by Roger Z. George and James B. Bruce. Washington, D.C.: Georgetown University Press, 2008.

"The Loyalty Oath Controversy, University of California 1949-1951." Berkeley: Regents of the University of California, 2006.

Mandelbaum, Michael. *The Nuclear Revolution Cambridge*. Cambridge: Cambridge

University Press, 1981.

Mandelbrot, Benoit , Michael Frame, and Nial Neger. "Fractal Geometry." New Haven, CT: Yale University.

Masse, Todd, Siobhan O'Neil, and John Rollins. "Fusion Centers: Issues and Options for Congress." Washington DC: Congressional Research Service, 2007.

Maxwell, Robert. "Chief Bratton and Jim Wiatt: Friends Help L.A.'S Top Lawman Keep This City Safe." *Los Angeles Times*, 7 June 2009.

Mayer, Jane. "The Hidden Power: The Legal Mind Behind the White House's War on Terror." *The New Yorker*, 2006.

McConnell, Mike. "Overhauling Intelligence." *Foreign Affairs*, no. July/August (2007).

McKeever, Kent, and Last Updated. "Researching Public International Law." *Arthur W. Diamond Law Library Research Guides* (2006), http://www.law.columbia.edu/library/Research_Guides/internat_law/pubint#Definition%20of%20International%20Law.

Meselson, Matthew. "Averting the Hostile Exploitation of Biotechnology." *CBW Conventions Bulletin* 48, no. June (2000): 16-19.

Miller, Eugene F. "Leo Strauss: Philosophy and American Social Science." In *Leo Strauss, the Straussians, and the American Regime*, edited by Kenneth L. Deutsch and John A. Murley. New York: Rowman & Littlefield, 1999.

———. "Positivism, Historicism, and Political Inquiry." *The American Political Science Review* 66, no. 3 (1972): 796-817.

Morgan. *Domestic Intelligence: Monitoring Dissent in America*. Austin and London: University of Texas Press, 1980.

Morrow, Lance. "The Case for Rage and Retribution." *TIme Magazine*, 14 September 2001.

Moskos, Peter. "The Better Part of Valor: Court-Overtime Pay as the Main Determinant for Discretionary Police Arrests." *Law Enforcement Executive Forum* 8, no. 3 (2008): 77-94.

Nakashima, Ellen. "Fbi Shows Off Counterterrorism Database." *Washington Post*, 30 August 2006.

Napolitano, Janet. "Remarks to the National Fusion Center Conference." Kansas City, MO: Department of Homeland Security, 2009.

"National Intelligence Council Mission." http://www.dni.gov/nic/NIC_about.html.

"National Intelligence Estimate on Iraq's Continuing Program for Weapons of Mass Destruction." 2002.

"National Intelligence Strategy of the United States of America." Office of the Director of National Intelligence, 2005.

"National Security Act of 1947 (50 U.S.C. 403-3 (D)(1))."

"National Strategy for Combating Terrorism." edited by Homeland Security. Washington DC: White House, 2006.

"Nationwide Suspicious Activities Reporting Initiative: Fact Sheet." edited by Program Manager for the Information Sharing Environment (PM-ISE): Office of the Director of National Intelligence, 2008.

Nenneman, Milton. "An Examination of State and Local Fusion Centers and Data Collection Methods ", Naval Postgraduate School, 2008.

The New Oxford American Dictionary. New York: Oxford University Press, 2005.

Nicholas B, King. "The Influence of Anxiety: September 11th, Bioterrorism, and American Public Health." *Journal of the History of Medicine* October, no. 58 (2003).

Nietzsche, Friedrich Wilhelm. *Beyond Good and Evil: Prelude to a Philosophy of the Future*. Translated by Walter Kaufmann. New York: Vintage Books, 1966.

Noble, Ronald K. "70th Interpol General Assembly 24-28 September 2001." INTERPOL.

———. "Bio-Terrorism Conference 1st Interpol Global Conference, 1-2 March." INTERPOL.

Noon, David Hoogland. "Operation Enduring Analogy: World War Ii, the War on Terror, and the Uses of Historical Memory." *Rhetoric & Public Affairs*,no. 3 (2004).

O'Neil, Siobhan. "Terrorist Precursor Crimes: Issues and Options for Congress." Congressional Research Service, 2007.

Orlov, Aleksandr Ivanovich. *Handbook of Intelligence and Guerrilla Warfare*. Ann Arbor: University of Michigan Press, 1963.

"Oxford English Dictionary." Oxford University Press, 2005.

Palmer, Alyson M. "The Legal Questions Behind the Tb Case." In *law.com*: Incisive Media US Properties, 2007.

Parker, Charles F., and Eric K. Stern. "Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise " *Foreign Policy Analysis* (2005).

Patton, Paul. "The World Seen from Within: Deleuze and the Philosophy of Events." *Theory and Event*,no. 1 (1997), http://muse.jhu.edu/journals/theory_and_event/v001/1.1patton.html.

Peterson, Marilyn. "Intelligence-Led Policing: The New Intelligence Architecture." edited by Department of Justice: Bureau of Justice Assistance, 2005.

Prange, Gordon W. *At Dawn We Slept: The Untold Story of Pearl Harbor*. New York: McGraw-Hill, 1981.

Prange, Gordon W., Doland M. Goldstein, and Katherine V. Dillon. *Pearl Harbor: The Verdict of History*. New York: McGraw-Hill 1986.

Price, Richard. "A Genealogy of the Chemical Weapons Taboo." *International Oganization* 49, no. 1 (1995): 73-101.

"Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Assessment ". Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, 2008.

"Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare." Geneva, 1925.

Rabinow, Paul. *Anthropos Today: Reflections on Modern Equipment*. Princeton: Princeton University Press, 2003.

———. *French Modern. Norms and Forms of the Social Environment*. 2nd ed. Chicago / London: University of Chicago Press, 1995.

———. *Marking Time: On the Anthropology of the Contemporary*. Princeton: Princeton University Press, 2008.

Rabinow, Paul, and Gaymon Bennett. *A Diagnostic of Equipmental Platforms*. Berkeley: Anthropology of the Contemporary Research Collaboratory, 2007.

———. *Synthetic Anthropos: Designs for Human Practice*: Connexions, 2008.

"Racial Profiling." *Police Assessment Resource Center* (2009).

Rafter, Nicole Hahn. *Creating Born Criminals*. Urbana: University of Illinois Press, 1997.

Rankin, Bill. "Ex-Tech Student Found Guilty on Terrorism Charge. Father: Ahmed 'Not Guilty of Any Crimes in the Eyes of Allah'." *Atlanta Journal-Constitution* 2009.

———. "Terror Trial Verdict: Guilty." *Atlanta Journal-Constitution*, 2009.

Ransom, Harry Howe. "Review: Strategic Intelligence and Foreign Policy " *World Politics* 27, no. 1 (1974): 131-46.

Ratcliffe, Jerry H. "Intelligence-Led Policing." In *Environmental Criminology and Crime Analysis*, edited by Richard Wortley, Lorraine Mazerolle and Sacha Rombouts, 263-82. Portland, USA and Devon, UK: Willan Publishing, 2008.

"Report of the Senate Select Committee on Intelligence on the U.S. Intelligence Community's Prewar Intelligence Assessements on Iraq Together with Additional Views." 523. Washington, DC, 2004.

"Report on the Investigative Data Warehouse ". edited by Electronic Frontier Foundation, 2009.

"Report to Congress Regarding the Terrorism Information Awareness Program: Detailed Information." Department of Defense, 2003.

Rice, Condoleezza. "Transcript of Dr. Conoleezza Rice's 9/11 Commission Statement Wednesday, May 19, 2004." CNN, http://www.cnn.com/2004/ALLPOLITICS/04/08/rice.transcript/.

Richards J. Heuer, Jr. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence: CIA, 1999.

Riedel, Stefan. "Biological Warfare and Bioterrorism: A Historical Review." *Baylor University Medical Center Proceedings* 17, no. 4 (2004): 400–06.

Rieff, David. "Policing Terrorism." *New York Times*, 22 July 2007.

Riley, K. Jack, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis. "State and Local Intelligence in the War on Terrorism." In *RAND Infrastructure, Safety, Environment*, 2005.

Risen, James. "In Hindsight, C.I.A. Sees Flaws That Hindered Efforts on Terror." *New York Times*, 7 October 2001.

Risen, James, and David Johnston. "Officials Say They Saw No Signs of Increased Terrorist Activity." *New York Times*, 12 September 2001.

Roosevelt, Franklin D. "7 December Proposed Message to the Congress." http://www.archives.gov/education/lessons/day-of-infamy.

Rosenberg, Emily S. *A Date Which Will Live: Pearl Harbor in American Memory*. Edited by Gilbert M. Joseph and Emily S. Rosenberg, American Encounters / Global Interactions. Durham: Duke University Press, 2003.

Rowley, Coleen M. "Oversight Hearing on Counterterrorism, Senate Committee on the Judiciary." Washington, D.C.: FBI, 2002.

Rumbaut, Rubén G., and Egon Bittner. "Changing Conceptions of the Police Role: A Sociological Review " *Crime and Justice* 1 (1979): 239-88.

Rusen, Jorn. "Rhetoric and Aesthetics of History: Leopold Von Ranke." *History and Theory* 29, no. 2 (1990): 190-204.

Sample, Timothy R. "A Federal Approach to Domestic Intelligence." In *Vaults, Mirrors, and Masks : Rediscovering U.S. Counterintelligence*, edited by Jennifer E Sims and Burton L Gerber. Washington, D.C.: Georgetown University Press, 2009.

Schelling, Thomas C. "Foreword." In *Pearl Harbor: Warning and Decision*, vii-ix. Stanford: Sanford University Press, 1962.

Schmitt, Eric. "Surveillance Effort Draws Civil Liberties Concern." *New York Times*, 29 April 2009.

Schmitt, Eric, and Thom Shanker. "U.S. Adapts Cold-War Idea to Fight Terrorists." *International Herald Tribune*, Tuesday, 18 March 2008.

Schmitt, Francis O. "Contributions of Molecular Biology to Medicine." *Bull N Y Acad Med* 36, no. 11 (1960): 725–49.

Schmitt, Gary. "Our Basic Instincts Were Sound." *Los Angeles Times*, 1 February 2004.

Schmitt, Gary J. "Truth to Power? Rethinking Intelligence Analysis." In *The Future of American Intelligence*, edited by Peter Berkowitz, 41-64. Stanford: Hoover Institution Press, 2005.

Schmitt, Gary J., and Abram N. Shulsky. "Leo Strauss and the World of Intelligence (by Which We Do Not Mean Nous) " In *Leo Strauss, the Straussians, and the American Regime*, edited by Kenneth L. Deutsch and John A. Murley, 407-12. New York: Rowman & Littlefield, 1999.

Schneier, Bruce. "Terrorists Don't Do Movie Plots." *Wired*, 8 September 2005.

Schulte, Brigid. "As Age of Apocalypse Dawned, So Bloomed a Bunker Mentality " *The Philadelphia Inquirer*, 20 August 1995.

Seifert, Jeffrey W. "Data Mining and Homeland Security: An Overview." Washington DC: Congressional Research Service, 2007.

———. "Data Mining and Homeland Security: An Overview (Updated)." Washington DC: Congressional Research Service, 2008.

Shane, Scott, and Lowell Bergman. "Contained? Adding up the Ounces of Prevention." *New York Times*, 10 September 2006.

Shulsky, Abram N., and Gary J. Schmitt. *Silent Warfare: Understanding the World of Intelligence*. 3rd ed. Dulles: Potomac Books, 2002.

Smith, Gregory Bruce. "Athens and Washington: Leo Strauss and the American Regime." In *Leo Strauss, the Straussians, and the American Regime*, edited by Kenneth L. Deutsch and John A. Murley. New York: Rowman & Littlefield, 1999.

Smith, Richard Harris. *Oss: The Secret History of America's First Central Intelligence Agency*. Berkeley,: University of California Press, 1972.

"State and Local Fusion Centers." Washington, D.C.: Department of Homeland Security, 2009.

Steinberg, James B. "The Policymaker's Perspective: Transparency and Partnership." In *Analyzing Intelligence: Origins, Obstacles, Ad Innovations*, edited by Roger Z. George and James B. Bruce, 82-90. Washington, D.C.: Georgetown University Press, 2008.

Steury, Donald P. "Introduction." In *Sherman Kent and the Board of National Estimates : Collected Essays*, edited by Donald P. Steury. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1994.

Strauss, Leo. *Natural Right and History*, Charles R. Walgreen Foundation Lectures. Chicago: University of Chicago Press, 1953.

———. *On Tyranny*.

———. *Persecution and the Art of Writing*. Glencoe, Illinois: Free Press, 1952.

"Subject: Field Contacts, Number: 402/21." edited by State of Texas Alamo Community Colleges Police, 2008.

Suettinger, Robert L. "Overview: History of Intelligence Analysis." (2004), http://www.dni.gov/nic/NIC_tradecraft_overview.html.

Taipale, K. A. "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data." *Columbia Science and Technology Law Review* V (2003).

110th Congress. *To Provide for the Implementation of the Recommendations of the National Commission on Terrorist Attacks Upon the United States*. 1st Session, H.R.1 Public Law No: 110-53.

"Training Bulletin : Automated Information Systems V-C.2 Calea Ref No. 81.2.9, 82.3.6, 82.3.8." Oakland Police Department, 2000.

Travis, Alan. "Mi5 Report Challenges Views on Terrorism in Britain." *Guardian*, 20 August 2008.

———. "Terror Law Used to Stop Thousands 'Just to Balance Racial Statistics'." *Guardian*, 17 June 2009.

Trebilcock, Craig T. "The Myth of Posse Comitatus." *Journal of Homeland Security* October (2000).

Treverton, Gregory F. "Intelligence Analysis: Between "Politicization" And Irrelevance." In *Analyzing Intelligence: Origins, Obstacles and Innovations*, edited by Roger Z. George and James B. Bruce. Washington, D.C.: Georgetown University Press, 2008.

Tucker, Jonathan B. "A Farewell to Germs: The U.S. Renunciation of Biological and Toxin Warfare." *International Security* 27, no. 1 (2002): 107-48.

United States Department of Justice Et Al. V. Reporters Committee for Freedom of the Press Et Al. 489 U.S. 749, (1989).

"Vertic: About the Centre."

Vogel, Kathleen. "Framing Biosecurity: An Alternative to the Biotech Revolution Model?" *Science and Public policy* 35, no. 1 (2008): 45-54.

Wagner, Dan. "Forward : Sherman Kent and the Profession of Intelligence Analysis." *The Sherman Kent Center for Intelligence Analysis Occasional Papers*,no. 5 (2002).

Walker, David A. "Oss and Operation Torch " *Journal of Contemporary History* 22 no. 4 Intelligence Services during the Second World War: Part 2 (1987): 667-79.

Ward, Kenneth D. "The Bwc Protocol: Mandate for Failure " *Nonproliferation Review* Summer (2004).

Warner, Michael. "The Office of Strategic Services: America's First Intelligence Agency." *Books and Monographs of United States Central Intelligence Agency*,no. May (2000), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/oss/index.htm.

Weber, Max. "Objectivity in Social Science and Social Policy " In *The Methodology of the Social Sciences*, edited by E. A. Shils and H. A. Finch. New York: Free Press, 1904 (1949).

———. "Science as a Vocation." In *From Max Weber: Essays in Sociology*, edited by H. H. Gerth and C. Wright Mills. New York: Oxford University Press, 1946.

"What You Should Know About Biological Warfare ". 7:17. USA: U.S. Federal Civil Defense Administration, 1952.

Winks, Robin W. *Cloak & Gown : Scholars in the Secret War, 1939-1961*. 2nd ed. New Haven: Yale University Press, 1996.

Wirtz, James J. "Responding to Surprise." *Annual Review of Political Science*,no. 6 April (2006).

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford: Sanford University Press, 1962.

———. "Signals and Noise: The Intelligence Picture." In *Pearl Harbor: Roosevelt and the Coming of the War*, edited by George Macgregor Waller, 83-94. Boston: Heath, 1965.

Wright, Susan. "Terrorists and Biological Weapons: Forging the Linkage in the Clinton Administration." *Politics and the Life Sciences* 25, no. 1-2 (2007): 57-115.

Yoo, John C. "September 25, 2001 Memorandum Opinion for the Deputy Counsel to the President: The President's Constitutional Authority to Conduct Military Operations against Terrorists and Nations Supporting Them." edited by Department of Justice. Washington, D.C.: Office of Legal Counsel, 2001.

Zegart, Amy. "9/11 and the Fbi: The Organizational Roots of Failure " *Intelligence & National Security* no. 2 (2007).

———. "Our Clueless Intelligence System." *Washington Post*, 8 July 2007.

———. "September 11 and the Adaptation Failure of U.S. Intelligence Agencies." *International Security*,no. 4 (2005).