Journal of Political Sciences & Public Affairs
ISSN: 2332-0761

Hastedt, J Pol Sci Pub Aff 2015, 3:3
DOI: 10.4172/2332-0761.1000178

Research Article Open Access

NSA Intelligence Gathering: An Organization Theory Perspective

Glenn Hastedt*

James Madison University, Harrisonburg VA, VA, USA

Abstract

Significant obstacles standing in the way of advancing our knowledge of the operation of intelligence organizations is the difficulty of obtaining reliable information. The veil of secrecy surrounding their operations makes both in-depth single event case studies and comparisons across time or countries difficult to assemble. Consequently these studies typically are centered on situation specific personality and politics driven narratives. All too often unexamined is the possibility that the actions of intelligence agencies are fully consistent with the underlying logic of decision making found in the organization theory literature. To the extent that this is the case intelligence organizations can be treated as "normal" organizations with predictable tendencies. Presented here is an exploratory analysis using organization theory to understand the actions of one intelligence agency, the National Security Agency.

Keywords: National Security Agency; Organization theory; Intelligence

Introduction

Constructing empirical explanations and normative assessments of controversial actions carried out by intelligence organizations is no easy task. The veil of secrecy surrounding their operations makes both in-depth single event case studies and comparisons across time or countries difficult to assemble. Consequently these studies typically are centered on personality and politics driven narratives in which the uniqueness of the intelligence organizations are stressed: the key role perceptions and historical experience; good guys vs. bad guys; conspiracy theories driven by back room and secret negotiations; organizations out of control or being overly aggressive in carrying out their mission; one set of politicians opposing another. Most famously these competing explanatory frameworks emerged during the Watergate hearings when Senator Frank Church initially labelled the CIA to be a "rogue elephant" while the Pike Committee concluded that the CIA had not undertaken major actions without approval from high ranking policy makers. To a considerable degree, media narratives on the warrantless electronic surveillance program revealed by Edward Snowden's leaking of National Security Agency (NSA) documents in 2013 repeated this pattern with the NSA alternately portrayed in the media as an organization out of control and one doing the bidding of policy makers.

Obscured by these competing characterizations is the possibility that the actions of intelligence agencies are fully consistent with the underlying logic of decision making found in the organization theory literature. To the extent that this is the case intelligence organizations can be treated as "normal" organizations with predictable tendencies. What follows is an exploratory analysis using organization theory to understand the actions of one intelligence agency, the NSA. It proceeds in four parts. First, I present an organization theory framework to use in analyzing NSA actions. Second, I present a historical overview of the NSA's actions in the context of this framework. Third, I examine the NSA's response to the Snowden revelations. Fourth, I present concluding thoughts on the importance of using theoretical frameworks to examine the actions of intelligence organizations.

Organizational Architectures

No single theory of organizations exists to draw upon in identifying insights into the operation of intelligence organizations. The approach followed here is to examine the operation of the NSA's electronic surveillance program from a perspective found in the classic literature on organization theory which holds that organizations are best seen as open, problem facing- problem solving systems [1-3]. The central challenge facing organizations from this perspective is one of responding to uncertainty in their operating or task environment with a standard organization response being to manipulate and control their environment rather than change organizational behavior [4]. To be effective as problem facing-problem solving units, organizations must undertake actions based on the criteria of rationality [5-8]. First, they need to organize their internal activities in such a way as achieve the desired outcomes. Organizational culture is a major internal constraint on these efforts since to a considerable extent they evolve from outside of the control of organizational leaders. Second, they need to put into place external boundaries around the organization that protect core processes from being undermined by disruptions and uncertainties in the environment. One of the most significant potential threats facing an organization is that it can become so dependent on some elements of its environment for resources that it can lose its ability to function effectively. Faced with such threats organizations will seek to minimize the power held over them by elements of its environment by maintaining alternatives, acquiring prestige, coopting threatening forces, forming coalitions with them, reaching understandings as to the nature of permissible actions (contracting), and, if all else fails, enlarge its task environment to bring new forces into play that can offset the influence of those who threaten it. Third, organizations need to shape the evaluation criteria used to assess their performance. As problem facing-problem solving units, organizations undergo constant external and internal evaluations as to their current performance and fitness for the future. The selection of standards by which to assess performance thus becomes a going issue of concern. General standards of desirable behavior emanating from societal values provide one benchmark for evaluating organizational performance. The ambiguity typically found here as well as the often impractical nature of these standards often limits the utility of societal values as the sole or primary source of standards.

***Corresponding author:** Glenn Hastedt, James Madison University, Harrisonburg VA, VA, USA, Tel: 540-568-6211; E-mail: hastedgp@jmu.edu

Received September 17, 2015; **Accepted** October 15, 2015; **Published** October 25, 2015

Citation: Hastedt G (2015) NSA Intelligence Gathering: An Organization Theory Perspective. J Pol Sci Pub Aff 3: 178. doi:10.4172/2332-0761.1000178

In light of this organizations turn to measures of success which are more concrete yet at the same time offer them a significant degree of control over how they are formulated and applied. Such measures include demonstrating past efficiency, historical improvement, positive comparisons with other organizations, and extrinsic or symbolic measures of fitness for future action.

NSA's Architecture: Ongoing Environmental Turbulence

Except for periodic outbursts of unwanted public attention, the NSA has largely succeeded in operating behind a wall of secrecy. The absence of news has helped promoted a public image of the NSA as an effective smoothly functioning organization fully in control of its environment. Yet looking beneath the surface reveals that NSA faced its share of challenges and in responding to them has behaved in a manner predicted by organization theory. Perhaps the most significant challenge facing the NSA since its establishment in 1952 is that its external task environment has been anything but stable in spite of the underlying continuity in its priority intelligence mission of providing warning, strategic, and tactical intelligence on the Soviet Union. Both the cold war and post-cold war periods contained within them a series of short term crises and long term conflicts. The cold war saw a series of crises over Berlin, the outbreak of war in Korea, the Cuban Missile crisis, decolonization in Africa, a series of Arab-Israeli conflicts, the fall of the Shah, the Soviet invasion of Afghanistan, conflicts in Central America, and the Vietnam War. The post-cold war period has seen the 9/11 terrorist attacks and the ensuring global war on terrorism, aggressive action by China and Russia to establish regional dominance, domestic unrest and international interventions growing out of the Arab Spring, and U.S. foreign policy missteps in Haiti, Bosnia, and Somalia. Taken as a whole these events have presented significant intelligence challenges for the NSA and other intelligence agencies. Often these intelligence agencies correctly alerted policy makers to impending problems such as weeks before the Pueblo was attacked by North Korea the NSA issued a warning that called for U.S. ships to begin taking protective measures or in the lead up to the Soviet invasion of Afghanistan when the NSA predicted it would occur. But these successes and others conceal an underlying reality. Intelligence resources are not like money. They cannot be spent with equal effectiveness on any problem. New or unanticipated intelligence problems demand intelligence resources that cannot be generated overnight**.** Intelligence surprises are thus to some extent inevitable and bring with them the potential challenges to organizational reputations and operations. President Dwight Eisenhower is described as unhappy that the first news he received about Joseph Stalin's death came from the Associated Press, A decade later the NSA's inability to read high-level Soviet ciphers contributed the NSA's ability to alert policy makers to Russia's plan to put missiles in Cuba. Only the NSA provided any advance warning of the Tet Offensive and then its SIGINT did not anticipate the true size and objective of the North Vietnamese attack. During Operation Desert Storm the ability of SIGINT to provide strategic and tactical intelligence was hindered by the absence of Arabic linguists. A similar scenario took place in the Iraq War where less that 2 percent of the military's tactical SIGINT messages were processed [9]. Technology is the second contributing factor to the ongoing turbulence of the NSA's task environment. Viewed with the benefit of 20-20 hindsight most scientific and technological breakthroughs seem foreordained or inevitable. Yet, the timing of scientific and technological advancements is anything but evenly spaced through time. Moreover, the ability of technology to solve problems is not permanent but can be limited (or enhanced) by a myriad of factors. Information from a spy caused the Soviet Union to change its codes thereby nullifying the ability of U.S. intelligence services to read Soviet military and internal security radio ciphers leading Bamford to comment that "in the middle of the Cold War, NSA had suddenly become hard of hearing" [10]. Not only did Soviet ciphers remain unbroken but reading high level Chinese communications was also largely beyond its reach. When NSA did score a major breakthrough in 1977 it was the result of sloppy work by Soviet cipher system operators which allowed it to reconstruct parts of the Soviet military cipher system and read portions of the communication traffic. Technological challenges to intelligence also were a reoccurring theme in the war against terrorism as it played out in Afghanistan and Iraq. As in the past processing data was a problem. A navy study found that 60 percent of the data collected by NSA strategic SIGINT units was archived and never analyzed. Another study found that the army's tactical intelligence collection system was ill-suited for fast-moving offensive operations. Military commanders instead found themselves relying heavily on the NSA's national SIGINT system to local Iraqi Republican Guard units. In the end the army and marines junked much of their expensive SIGINT in favor of low end, commercially produced off- the-shelf radio scanners. Most recently the use of drones to provide intelligence information is presenting challenges to intelligence organization. 2015 found the army conducting 65 combat drone patrol mission per day. At the same time it was confronting problems of stress by those directing these missions and Pentagon plans to increase the use of drones by about 50% due to concerns about Russia and China as well as the need for more drones in Iraq and Syria. One acknowledged problem presented by such projected increases in the use of drones is that of processing and analyzing the additional flow of video and other forms of data [11]. A third area of turbulence in the NSA's task environment is found in repeated fluctuations in the operating resources allocated to it [10]. Prior to its creation President Harry Truman's rapid demobilization of the military following Japan's surrender resulted in army and navy COMINT organizations losing 80 percent of its workforce. By the end of 1945 code breaking had virtually ceased. Budgetary changes began to take place in the mid-1950s. The NSA's budget rose to $500 million, more than half the total allocated to the entire intelligence community. By the beginning of the Kennedy administration found the NSA operating in a very different budgetary environment. It had a budget of $654 million and employed 59,000 military and civilians. In contrast, the CIA's budget was $401.6 million with 16,685 employees. The budgetary pendulum swung back the opposite direction when Richard Nixon became president. During his presidency the intelligence community's budget fell by 40 percent and its workforce fell by 50 percent. The NSA was among the hardest hit losing one-third of its budget and seeing its staff fall from 95,000 in 1969 to 50,000 by 1980. Budgetary growth returned under Presidents Jimmy Carter and Ronald Reagan. NSA's budget quadrupled during the tenure of Vice Admiral Bobby Inman as NSA's director causing it to move from an organization "with a serious inferiority complex" to one that had "a corner on the market." Especially significant were increases Inman obtain to modernize NSA's global SIGINT satellite coverage. Under his successor, General Lincoln Faurer, NSA's workforce grew by 27 percent from 1981-1985. The end of the Cold War brought another reversal to the NSA's fortunes. President George H.W. Bush and Congress quickly moved to cut the intelligence community's budget reducing it by 16 percent from 1990-1995. Personnel layoffs in NSA followed and the number of its spy satellites was cut in half. Compounding matters was a 1991 internal NSA study that found it to be an effective organization but not an efficient one. Hoping to preempt further staffing and budgetary cutbacks in 1992 NSA director Vice Admiral James McConnell acted

preemptively to reorganize the NSA and trim its staff. NSA's operating budget surged again with the war on terrorism. Data contained in documents released to the press place the NSA's 2013 budget at $10.8 billion, a 53 percent increase since 2004. In terms of expenditures, the NSA spends $21.5 billion on data collection, $1.5 billion on data analysis, $5.2 billion on management, facilities and support, and $1.6 billion on data processing and exploitation. Estimates of NSA's workforce are often placed at about 40,000 people. The potential for more budgetary turbulence remains. In July 2013 the House by a vote of 217-205 narrowly defeated an amendment to a defense spending bill that would have ended NSA's authority to use section 215 of the Patriot Act to collect intelligence. NSA Director Alexander spent hours on the Hill lobbying members behind closed doors not to cut this funding. Closely related to the NSA's budgetary turbulence has been the periodic intervention of intelligence overseers into its affairs. Not surprisingly, the most frequent intrusions have come from the White House and have focused both on specific intelligence collection and analytical efforts, and broad-based evaluations of NSA performance. Also not surprisingly, political criteria were the dominant yardstick used. Most notable here were the Gulf of Tonkin, KAL 007, Iraq's invasion of Kuwait, and Iraqi WMD incidents in which the commitments to policy short-circuited intelligence. The lack of clarity inherent in such intrusions is conveyed by Matthew Aid's twin observations that by mid-1966 SIGINT in Bosnia had come to an almost complete standstill and that nonetheless senior Clinton administration officials "marveled" at NSA's ability to produce "one hot intelligence scoop after another" [9]. The Foreign Intelligence Surveillance Court (FISC) seldom intruded into NSA's task environment prior to 9/11. One exception occurred in 2000 when it tightened restrictions designed to better separate FBI criminal investigations employing electronic eavesdropping and NSA national security intelligence gathering operations. Under the new rules put into place before the NSA could pass information on to the FBI it would first have to determine the extent to which it contained information from its FISA surveillance. The NSA responded to this added requirement by shifting the burden of authorization to the FBI of determining if this was the case by inserting a blanket warning statement on all information related to terrorist activities that this might be the case on all information passed on. Intrusions by Congress into NSA's task environment were infrequent but significant events for the NSA since they often took the form of public hearings and inquiries undertaken in the wake of revelations of NSA wrongdoings, foreign policy failures, and national tragedies. The first of these experienced by the NSA was the Church Committee hearings into domestic spying by the intelligence community that led to the creation of permanent House and Senate intelligence committees as well as the FISC.

The NSA's Patterned Response to Organizational Turbulence

Throughout its history the NSA responded to this environmental turbulence in a consistent and predictable manner that was in accordance with the expectations of organization theory. The strategy it employed had three parts: 1) collecting data and lots of it, 2) coopting and controlling key technologies, and 3) neutralizing the influence of keying oversight agencies. Former NSA director Lt. Gen. Keith Alexander in responding to stories of Snowden's leaks on NSA intelligence gathering operations put this outlook in quite simple terms: "you need a haystack to find a needle" [12]. The NSA did not invent the strategy of building a bigger haystack. As WW II ended, army and navy intelligence were reading the cipher machines from 60 countries, a number far in excess of the number of Axis sympathizers and puppet states controlled by Germany, Italy and Japan. When U.S. COMINT agencies encountered difficulty breaking the Russian code they turned to an alliance with Great Britain in the form of the British-United States Communication Intelligence Agreement to standardize and improve intelligence sharing between the two countries. Subsequently a number of other agreements were entered into but they did not all carry the same obligations. For the Five Eye countries (U.S., U.K. Canada, Australia and New Zealand) the agreement was that they would not engage in espionage against each other. In other cases the agreements were limited to sharing signals intelligence or to providing NSA with signals intelligence in return for technology or cash. The immediate post WW II period saw a continued reliance on the technologies used to break encoded radio and telegraph communications. As these forms of communication began to be supplanted by data transmitted by satellites, the NSA began in the 1960s to develop a satellite intelligence collection system. The first intelligence gathering satellite was put in orbit in 1966. In 1981 the construction of a global system of intelligence satellites began. The capabilities of this system allowed it to look beyond the primary targets of Russia and other communist states to include transmissions by individuals and corporations. Changes in communications technologies in the early 21st century forced still another change in the NSA's collection system. Satellite communications were now largely replaced by fiber optic communications. Accessing data carried through them on a global scale requires tapping into underwater cables. It also required a FISC warrant which was not the case for satellite communications. The increased scope of NSA intelligence collection took many forms. When high level Russian and Chinese ciphers proved too challenging to read the NSA turned to the more aggressive gathering of low level communications. When North Vietnam improved the encryption of its high level communications the NSA obtained its best intelligence from reading the diplomatic cables from countries with embassies in Hanoi and by intercepting dispatches and communications from visiting journalists. As the George W. Bush administration was struggling to get United Nations support for the war against Iraq the NSA began monitoring "a large number of international organizations, all of whom were key players standing in the way" [9]. Establishing firm working relationships with other intelligence producers in its task environment was a key component of this for strategy of maximizing access to information. But, consistent with the expectations of organization theory for NSA cooperation coexisted with competition. This was the case even with its most valued Cold War ally, Great Britain. The two countries cooperated effectively on ECHELON but each withheld from the other knowledge of their own efforts to break Russian codes and a prime reason the U.S. was blind to the approaching Suez Crisis was that U.S. intelligence had ceded "ownership" of the Middle East to British intelligence. Additionally, a draft 2005 NSA document appears to give it the authority to act unilaterally and spy on British citizens [13]. In order to cordon off key technologies from environmental disturbances more was required than cooperation with allies. Securing the cooperation of communication companies was also essential. It was only through their cooperation that the full scope of international communications could be monitored. *Operation Shamrock* was established in 1945 with such cooperation. The Armed forces Security Agency acquired daily copies of all telegraph communications coming into and going out of the United States through Western Union, RCA Global and ITT World Communications. Their cooperation was not unreservedly given. To protect themselves from prosecution for they initially sought authorization from the U.S. attorney general. Although none was forthcoming they began providing copies of the desired communications. Company concerns continued

with the request now being that authorization come from the president. In 1949 they received this in the form of a memorandum from a meeting on the subject attended by Truman. The need to access fiber optic communications required a new effort by NSA to obtain the cooperation of commercial communication firms [14,15] The initial target was Qwest [16]. It proved uncooperative citing legal constraints including the provisions of the 1986 Electronic Communications Privacy Act which extended prohibitions on telephone wiretaps to electronic computer based information. NSA then turned to AT&T which had discovered a method for tapping into underwater fiber cables. Information obtained by Snowden released in 2015 revealed that from 2003 to 2013 AT&T provided the NSA with several billion emails. In 2011 it was providing NSA with over 1.1 billion cellphone calling records per day. In 2013 NSA was processing 60 million foreign-to-foreign emails per day [17]. Included in these intercept programs were communications involving Iran and allied terrorist groups [18]. AT&T and other firms had established an ongoing working relationship with the NSA through the National Security Advisory Board established in 1953 that provides the NSA with advice on research, development and application of new and existing technologies. Further cementing the alliance NSA established with communication firms is the Intelligence and National Security Alliance previously known as the Security Affairs Support Association made up of companies with which the NSA frequently enters into contracts with. Where Snowden's initial leaks of PRISM revealed the existence of an extensive system of collaboration between the NSA and communication companies, much remained unseen. In the eyes of some what had been created was a multidimensional intelligence-industrial complex that had been put together through a combination of jawboning, stealth, legal protections, and monetary rewards. Legal protection came in the form of the granting telecoms immunity from prosecution from any lawsuits brought against them for their having cooperated with government requests to turn over information. Jawboning took many forms. Appeals to patriotism played a central role. So too did indirect pressure when those appeals failed. As one Verizon executive noted, "At the end of the day, if the Justice Department shows up at your door, you have to comply" [19]. An intelligence official attributed their cooperation to a maturing of the IT community. Opening Washington offices and coming into closer daily contact with the government caused them to shed much of their "initial arrogance" and made them recognize they were now part of the country's infrastructure and needed to deal with the government. Stealth too operated a many levels. A 2003 Network Security Agreement with Global Crossing was soon followed by similar agreements with other telecom firms [16]. That agreement required Global Crossing to have a Network Operations Center in the United States so that within 30 minutes of warning intelligence officials could visit the site. Moreover, all surveillance requests had to be handled by U.S. citizens possessing security clearances. At the same time acting unilaterally the NSA was tapping into the fiber optic cables that connect their data centers worldwide and thereby gain a back door into their communication systems should front door agreements fail. A second stealth operation involved the SIGINT Enabling Project on which according to data leaked by Snowden the NSA had spent more than $250 million per year. Its purpose was to actively engage U.S. and foreign IT firms in discussing about technology development in order to "covertly influence and/or overtly leverage their commercial products' designs" so they might be exploited by the NSA for intelligence gathering." Monetary rewards were most evident in the NSA's rapidly expanding use of contracting and consulting firms. While originally seen as a surge capability they have become a permanent fixture: 70% of the intelligence budget ($56 billion out of $80 billion) now goes to private contractors. Booz Allen Hamilton (BAH) for whom Snowden worked, is one such contractor. Obama's DNI James Clapper is a former BAH executive. Mike McConnell who served as President Bill Clinton's NSA director, left to work for BAH and then returned to government service as George W. Bush's DNI and has since returned to BAH. Of its 25,000 employees, 75% hold security clearances and 50% hold top secret clearances.

For these firms the contracts have been significant. A six month five company contract with NSA for Trailblazer, designed to sort and analyze web traffic collected by it, was originally for $280 million. When the project was cancelled in 2006 because it failed to perform successfully, the cost had reached into the billions of dollars. In another case, a computer systems contract awarded to BAH by the Department of Homeland Security for $2 million escalated $124 million. BAH continued to receive extensions on this contract because it was determined the intelligence community did not have the in house capacity to carry out the assignment [16]. Constructing a haystack on occasion also required cooperation with other U.S. intelligence organizations. These interactions also produced pronounced conflicts. A lengthy list of examples can be found spanning the entirety of the NSA's history. From the very outset NSA was viewed with skepticism by the CIA and State Department. In the early 1960s CIA director John McCone had Richard Bissell conduct a study of the NSA to determine why it was having such difficulties cracking Russian codes. The late 1960s were characterized by Aid as "a never-sending series of brawls" between the NSA and virtually everybody else in official Washington" including the military and CIA [9]. The early 1970s saw the NSA and CIA in periodic conflict over the quality and timeliness of NSA intelligence. One case involved the lead-up to the 1973 Arab-Israeli War with NSA director Lew Allen vowing that in the future he would make sure that the NSA's interpretation of SIGINT would be presented when it differed from those of other agencies. During the Carter administration CIA director Stansfield Turner and NSA director Inman each worried about the other's obsession with secrecy and fought for control over the SIGINT satellite program. The 1980s saw Secretary of Defense Caspar Weinberger look with suspicion on the NSA's close relations with the White House with some in the Pentagon assessing the NSA to be a rogue elephant. In the years leading up to the 9/11 attacks the NSA and FBI differed over who had responsibility for gathering intelligence on communications with foreign terrorists inside the United States with one NSA official noting that "our cooperation with our foreign allies is a hellluva lot better than with the FBI" [9]. A running point of contention between the NSA and FBI was over its 1967 refusal to continue to aid the NSA by breaking into foreign embassies so that the NSA might establish wiretaps. Organizational responses to these cooperation-conflict standoffs followed the expected pattern: each organization sought to acquire the disputed capability thereby minimizing the need for cooperation. In the early 1950s the CIA uncertain over the NSA's performance potential sought to build its own SIGINT system. In the early 1960s the NSA sought to secretly build its own surveillance naval force to complement its SIGINT air force. Frustrated by what it saw as an overly controlling NSA in the command of ocean going surveillance vessels the navy sought its own ships, one of which would be the *Pueblo*. Interestingly, perhaps the most damaging decision made by NSA leaders was complying with a 1967 request from the army for intercepts of electronic communications of American citizens and groups opposed to the Vietnam War. In 1969, this program became known as MINARET. Along with the Defense Department other agencies receiving intercepted messages were the FBI, CIA, Secret Service, and Bureau of Narcotics. By the time it was terminated in 1973 MINARET had generated over 3,900 reports. To

rebuild relations with Congress following the Church Committee hearings Inman employed a strategy of providing access to NSA secrets as a tool for converting key congressional figures and committee members into allies. He followed a similar strategy in dealing with the press providing reporters with access to secret information which had the effect of reducing their inclination to produce negative headline making stories of the NSA's activities.

In the wake of revelations about ECHELON Hayden would be the next NSA director to face Congress. The political fallout the befell the NSA from this involvement and in ECHELON led Hayden to take a defensive and cautious approach to any NSA involvement in communications surveillance within the United States even though FISC procedures permitted it when specified conditions were met. Bamford describes his testimony as deliberately intended to disarm his opponents and that he did with great success, at least for a while. For example, while not all committee members agreed with Bush's authorization of a NSA warrantless electronic surveillance program they complained in private to administration officials [16]. An additional element of Hayden's strategy to build committee trust was to cut back considerably on NSA surveillance operations that if exposed could bring it a renewed spate of hostile press coverage and more congressional inquiries. This decision, made to protect the NSA rather than promote U.S. foreign policy objectives, is seen by some as contributing to the 9/11 attacks because it was not coordinated with the FBI or other agencies. Yet, the 9/11 Commission largely ignored the NSA in its report focusing instead on the CIA. Hayden's ability to keep the NSA out of the headlines came to an end in 2005 when the *New York Times* reported that in 2002 President Bush had authorized the NSA to conduct NSA to monitor international phone calls and emails without a warrant. This story broke the day before the Senate was to take a vote reauthorizing the PATRIOT Act. As the controversy over Bush's power to do so grew his administration sought to justify it on various grounds. First, they argued the authorization on constitutional grounds ("the constitution vests in the President inherent authority to conduct wireless intelligence surveillance of foreign powers or their agents"), then by citing the September 14, 2001 congressional joint resolution which authorized Bush to use "all necessary and appropriate force" to defeat al Qaeda, and finally citing the need for speed in collecting and assessing intelligence by defining the program as one of terrorist surveillance and citing a threat to crash a jetliner into a Los Angeles skyscraper . A strong lobbying campaign by the White House plus a renewed willingness to brief the intelligence committees on these programs effectively put an end to congressional support for an investigation. Rebuilding relations with political overseers was not the only reform strategy engaged in by Hayden. He also sought to better understand the NSA's culture with an eye to changing it. Upon assuming this position he organized two different groups, one composed of insiders and one of outsiders, to examine its inner workings and make recommendations for changes. The insider group called for attacking the existence of internal barriers to communication, characterized the NSA as an organization whose individual capabilities transcended its organizational capabilities, and spoke of an "insular, sometimes arrogant culture" [10]. Likewise, the outside team criticized its "secrecy driven culture." Hayden was succeeded by Lt. Gen. Keith Alexander who ordered another internal study. It concluded the NSA lacked a unity of purpose and an identity crisis. Fragmentation, it argued, had created a lack of trust within the organization [16].

The Snowden Leak and the NSA's Response

On June 5, 2013, the *Guardian* and the *Washington Post* reported on the existence of a secret domestic surveillance program. A ruling obtained by the NSA from the Foreign Intelligence Surveillance Court (FISC) directed Verizon Business Network Services to provide the NSA "on a daily basis" all call logs "between the United States and abroad" or "wholly within the United States, including local telephone calls." The directive did not include the content of the communications but only metadata: the beginning and end points of a communication and its length. The White House initially declined to comment but the following day it was confirmed by Director of National Intelligence James Clapper [20]. Edward Snowden, a 29 year old high school dropout working for the BAH was the source of the NSA leaks. Snowden indicated he did so because "the public needs to decide whether these programs and policies are right or wrong" [21]. With the Snowden leaks the NSA once again confronted the problem of limiting intrusions into its operations from overseers. The NSA and its supporters employed a full range of measures designed to protect its core technologies in responding to calls for terminating these programs or significantly altering how they were conducted. Clapper's initial response was to stress the legality of the program. He asserted that while the NSA might "incidentally acquire" about Americans and foreign residents it could not intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States [20]. Other NSA defenders cited Section 702 of the FISA Amendment Act of 2008 which allowed the Attorney General and Director of National Intelligence to jointly authorize targeting of non-U.S. persons reasonably believed to be outside of the United States for periods of up to one year and Section 215 of the 2007 PATRIOT ACT which allows the FBI to order individuals or entities to turn over tangible things that are relevant for an authorized investigation into terrorist or clandestine intelligence activities. The FBI does not need to show probable cause nor must it believe that the person under investigation is a foreign power or agent of a foreign power. Individuals or entities served with Section 215 orders are not permitted to reveal this. Those subject to surveillance are not informed. This legal defense came under attack on two fronts. First, the lack of specificity in the language authorizing legislation was cited. These documents contained terms such as "targeted" and "tangible things" It was argued that this permitted the NSA to obtain larger amounts of data than it should have. This criticism was reinforced by the leaking of an internal NSA audit citing cases where it had violated these rules and an FISC court finding that one of its collection programs was "deficient on statutory and constitutional grounds" [22]. Second, the extent of oversight was challenged. According to some members of the intelligence and judiciary committees, intelligence oversight hearings on the telephone surveillance program in 2010 and 2011 were largely one sided sessions with few details being given unless a precisely worded question was put forward. Committee members also cited difficulties in gaining information from classified materials. They could only be read in secure offices, they could not takes notes with them when they left, and they were not permitted to discuss the issues with colleagues, staff members or outside experts. Concerns about its oversight capabilities were also expressed by members of the FISC. Judge Reggie Walton observed that the court lacked "the capacity to investigate issues of noncompliance" [23]. Former FISC judge James Carr noted "there were several occasions when I and other judges faced issues none of us had encountered before" [24]. Along with a legal defense came efforts at political protection. Neither President Obama nor Congressional leaders in both parties showed much interest in opening investigations into its actions. Boehner expressed confidence that "there is heavy oversight of this program" in the Congress [25]. To the extent that he expressed any criticism at all it was directed at President Obama for not being more

forceful in explaining how vital the NSA program was to U.S. security. Sen Saxby Chambliss, vice chair of the Senate Select Intelligence Committee, said of the NSA program, it has "proved meritorious, because we have gathered significant information on bad guys and only bad guys over the years" [26]. Diane Feinstein, chair of the Senate Select Committee on Intelligence, praised NSA director James Clapper who the previous year in response to a direct question by Sen. Ron Wyden if the NSA had collected any type of data on millions or hundreds of millions of Americans replied "no sir." Clapper later apologized for the statement saying he had not thought of Section 215 of the Patriot Act. As public pressure mounted congressional supporters Congress altered their strategy of passive defense and became proactive. One day after more NSA secret documents were released and accompanied by a statement from Snowden that the truth "is coming and cannot be stopped," the House Permanent Intelligence Committee convened a public hearing entitled "How Disclosed National Security Agency Programs Protect Americans, and Why Disclosure Aids Our Enemies." Committee Chair Mike Rodgers began the hearing by observing "it is at times like these when our enemies within become almost as damaging as the enemies on the outside' [27]. Among those testifying were NSA Director General Keith Alexander, Deputy Director of the FBI Sean Joyce, NSA Deputy Director Chris Iglis, Deputy Attorney General James Cole, and General Counsel to the Office of the Director of National Intelligence. Media accounts portrayed them as speaking from a common script that emphasized the NSA's program as having thwarted over fifty unsubstantiated terrorist attacks [27]. NSA and its supporters also engaged in a variety of rhetorical lines of defense to justify its actions. First to be employed was an effort to redirect blame away from the NSA and on to Snowden. Speaker of the House John Boehner quickly identified him as a "traitor" [25]. Senator Feinstein echoed that sentiment asserting that Snowden's leaking of secret NSA documents was an "act of treason" [28]. This theme was picked up again in early January 2014 by a classified Defense Intelligence Agency portions of which were leaked by congressional supporters in hopes of countering the impression that Snowden was a principled whistle-blower. The Government Accountability Project which serves as an advocacy organization for whistleblowers characterized its negative commentaries as "classic acts of predatory reprisal…that constitute retaliation." The goal is "to discredit the whistleblower by shifting the spotlight from the dissent to the dissenter when what truly matters is the disclosure itself" [29]. A second line of rhetorical defense built upon the argument that collecting data is largely a technical and professional matter. According to Hayden, "this isn't a drift net out there where we are soaking up everyone's communications we are going after very specific communications that our professional judgment tells us we have reason to believe are those associated with people who want to kill Americans" [29]. Hayden went on to cite "reasonableness as the operative professional standard. He continued noting that "to put someone on targeting under NSA anywhere in the world and at some point to end targeting doesn't mean that the first decision was wrong, it just means this was not a lucrative target for communications intelligence" [29]. The NSA's rhetorical defense of the surveillance program went on to include the vital role it played in protecting the United States that while short of concrete examples employed strongly symbolic imagery. Hayden quickly dismissed any notion of clemency for Snowden describing the NSA leaks as "the most destructive hemorrhaging of Americans secrets in the history of the Republic" [30]. Alexander at one point asserted that the NSA program had helped thwart dozens of potential attacks and at another time said it contributed to plot disruptions in over 90 percent of the cases. FBI Director Robert Mueller indicated that a larger version might have helped prevent the Boston Marathon attack [31]. Alexander and Representative Peter King argued the NSA program would have prevented the 9/11 attacks had it been in existence [32]. Critics challenged these assertions claiming no evidence had been produced to show that the NSA programs played a major role in stopping terrorism. While few details were given defenders did eventually cite a 2009 plot to attack the New York Stock Exchange and the conviction of four Somali immigrants in San Diego of conspiring to give support to al Shabaab [33]. The final element to the NSA's rhetorical defense of its surveillance program was to argue that it was standard procedure in the realm of national security. Senate Majority Leader Henry Reid observed, "everyone should just calm down and understand this isn't anything that is brand new" [34]. A senior administration official defended it as being line with NSA's mission: "their job is to get as much information for policymakers as possible" [35]. Dennis Blair who served as Obama's first DNI commented, 'if any foreign leader is talking on a cellphone or communicating on unclassified email, what the U.S. might learn is the least of their problems" [35]. Clapper observed that identifying the intentions of foreign leaders is a "fundamental given" for the operation of intelligence services [36]. Along these same lines 2007 NSA document released by Snowden asserted in the future, superpowers will be made or broken based on the strength of their cryptanalytic programs…It is the price of admission for the U.S. to maintain unrestricted access to and use of cyberspace" [37]. Still another rationale put forward compared the NSA's tracking of adversaries in cyber space with submarines. "That is what submarines do all the time they track adversary submarines [38]."

Conclusion

While the NSA's post-Snowden leak efforts to protect its core processes from environmental disturbances remains a work in progress placing them in the context of organization theory reveals several important points. Most important, there exists an underlying organizational logic to these actions. Efforts at collecting large quantities of data, developing new technologies that this might be possible, and cooperating with (and controlling) other countries, companies, and U.S. intelligence organizations was not haphazard responses or simply a product of the intelligence issue of the moment. They were a rational response to the environment the NSA operated in. Additionally, the NSA's ability to carry out this strategy as well as the shape it took reflected its organizational culture, a culture that instead of placing a check or restraint on this drive for data reinforced its pursuit along with the perceived technical nature of the mission. Finally, we see that consistent with organization theory's insights the NSA and its supporters advanced a series of evaluative criteria that while promoting a positive image of the NSA were often statement of opinion, unverifiable or lacking in specificity. Placing the operation of the NSA or the intelligence community in the context of a theoretical framework will not end disagreements over how to explain or evaluate its actions. Intelligence is too complex a subject for that to be the case. Personality and politics do matter. And, no consensus exists on what theoretical framework should be employed. What theoretical models allow us to do is move beyond the issues of the moment and examine the underlying forces at work and identify points of similarity over time. They offer the potential for establishing a firmer foundation on which to anticipate the future and develop policies to improve performance.

References

1. Thompson JD (1967) Organizations in Action. McGraw-Hill, New York.
2. James M, Simon H (1957) John Wiley, New York.
3. Richard C, March J (1963) A Rational Theory of the Firm. Prentice Hall,

Englewood Cliffs, N.J 32: 461-465

4. Galbraith JK (1973) Economics and Public Purpose. Houghton-Mifflin, New York.
5. Scott WR, Davis G (2007) Organizations and Organizing. Pearson, Englewood Cliffs, N.J.
6. Herbert K (1976) Are Governmental Organizations Immortal? Brookings, Washington, D.C.
7. Donald P, Warwick M (1975) A Theory of Public Bureaucracy. Harvard University Press, Cambridge, MA.
8. Hult Karen (2003) Environmental Perspectives on Public Institutions, in B. Guy Peters and Jon Pierre, eds., Handbook of Public Administration. Sage, London 149-161.
9. Matthew A (2009) The Secret Sentry. Bloomsbury Press, New York.
10. James B (2001) Body of Secrets. Anchor, New York.
11. Baldor L (2015) Pentagon Plans to Increase Deon flights by 50 Percent, New York Times, August 18.
12. Sanger D, Schmidt E (2013) N.S.A. Imposes Rules to Protect Data Stored on its Networks, New York Times, July 19.
13. Glanz J (2013) United States Can Spy on Britain Despite Pact, NSA Memo Says, New York Times, November 21.
14. Timberg C, Nakashima E (2013) Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance, Washington Post, July 6
15. Michael H (2013) How America's Top Tech Companies Created the Surveillance State, National Journal. July 25.
16. James B (2009) The Shadow Factory. Anchor, New York.
17. Angwin, J, Savage C , Larson J, Moltke H, Poitras L et al (2015) AT &T Helped U.S. Spy on Internet on a Vast Scale, New York Times, August 15.
18. Savage C (1015) N.S.A. Used Phone Records to Seek Iran Operatives, New York Times, August 12.
19. Perlroth N, Markoff J (2013) NSA May Have Hit Internet Companies at a Weak Spot, New York Times, November 26.
20. Savage C (2013) U.S. Confirms Gathering of Web Data Overseas, New York Times, June 7.
21. Mazzatti M (2013) Ex-Worker at CIA Says He Leaked Data on Surveillance, New York Times, June 9.
22. Savage C (2013) NSA Often Broke Rules on Privacy, Audit Shows, New York Times, August 16.
23. Leonning C (2013) Court: Ability to Police US Spying Program Limited, Washington Post, August 15.
24. Carr JG (2013) A Better Secret Court, New York Times, July 23.
25. Weisman J (2013) Boehner Calls Snowden Traitor. The New York Times, June 11, blog.
26. Mak T, Burgess E (2013) Diane Feinstein on NSA, Politico, June 6.
27. London E (2013) Congress, Intelligence Officials Join in Attacking NSA Whistleblower Snowden, World Socialist Web site, June 19.
28. Herb J, Sink J (2013) Sen. Feinstein Calls Snowden's NSA Leaks: 'an act of terror. The Hill, June 10.
29. Government Accountability Project (2014) "GAP Statement on Edward Snowden and NSA Domestic Surveillance." January 3.
30. Baker P (2014) Moves to Curb Spying Help Drive Clemency Argument for Snowden, New York Times. January 5.
31. Collins G (2013) The Other Side of the Story, New York Times, June 15.
32. Huetteman E (2013) Debating the N.S.A.'s Data Collection, and a Panel's Findings. The New York Times, December 22.
33. Pellerin C (2013) NSA Director: Security Leaks Have Done Great Harm, New York Times, June 14.
34. Weisman J (2013) As Criticism Grows, Curtailing Surveillance Program Seems Unlikely, New York Times, June 8.
35. Wilson S, Gearan A (2013) Obama Didn't Know About Surveillance of U.S.-Allied World Leaders Until Summer, Officials Say. The Washington Post, October 28
36. Schmidt M (2013) NSA Head Says European Data Collected by Allies. The New York Times, October 30.
37. Perlroth N, Larson J, Shane S (2013) NSA Able to Foil Basic Safeguards of Privacy on Web. The New York Times, September 5.
38. Sager D, Shaker T (2014) N.S.A. Devises Radio Pathway into Computers. The New York Times, January 14.