Globalization's Impact on Intelligence Failures:

Considerations for Reform in the U.S Security Clearance Model and

The Intelligence Community's Need for an Adaptation Culture

Jameson Crumpler

Journal of Homeland and National Security Perspectives Vol 5 No. 1 (2018)

The views expressed in this work are those of the author and do not reflect the official policy or positions of Angelo State University or the Center for Security Studies.

Abstract

Globalization has brought about tremendous forces of change to the US Intelligence Community (IC) in terms of divided individual allegiances and alliances and is imparting various impacts that will hinder the IC's ability to address these uncertainties unless the IC adopts an adaptation mindset, lest it faces yet another intelligence failure. Finding a way forward for the intelligence community and the national security clearance model will be a critically complex mission in support of US national security objectives.

Intelligence failure is perhaps one of the most widely studied elements within the broad field of intelligence and national security. Countless academic papers have been written, numerous presentations have been made on how to “improve intelligence” and avoid future failure. Government policy has made attempts to quell the tide of failure by enacting directives and implementing one of the largest government reorganizations since the creation of a national and centralized intelligence agency in 1947.

Failures in intelligence are not a new phenomenon. Such failures from intelligence itself and from the intelligence-policy process are issues with every intelligence service worldwide operating today. This phenomenon does not exist solely within the US Intelligence Community (IC).

In defining the phenomenon of “intelligence failure”, multiple definitions have been put forth by multiple authors, and near endless study has been made of some of the considerably major intelligence failures such as Pearl Harbor, and September 11th, 2001 (9/11). While these failures featured a “failure to warn” as their common denominator, there are many other types and examples of intelligence failure. These failures of intelligence range from missed opportunities that lead to the traumatic and tragic, to the seemingly more “mundane” of finding a US citizen has been spying for a foreign power, such as the Union of Soviet Socialist Republics (USSR, Soviet Union).

On defining intelligence failure, for example, in his academic paper “Intelligence Failure and Its Prevention” author Dwight M. Trafton proposes the definition of intelligence failure as borne of “preventable conditions”[1] such as an insufficient

1. Dwight E. Trafton, “Intelligence Failure and Its Prevention” (Naval War College, 1994), ii.

understanding of the methodologies used in analyzing intelligence and the various capabilities of intelligence as whole[2]. Trafton's definition is important because it reveals, contrary to popular belief (especially in the post-9/11 years), that intelligence failure does not only mean a failure to warn of a pending attack or a failure to predict a pending attack. Intelligence failure can arise at any level of the complex intelligence process and such failure can be strictly an "intelligence" failure (i.e. analytical failure), or an intelligence-policy failure (i.e. a policymaker fails to act on given intelligence) or a combination of both. The latter is usually the issue in most cases of intelligence failure.

Robert M. Clark, author of *Intelligence Analysis: A Target-Centric Approach*, opens his book with a discussion of why intelligence fails regarding the expectations we have placed upon intelligence because of human nature: the failure to share intelligence[3]. This one seems simple enough, but the simplest explanations are often ignored. This was evident in the Iraqi Weapons of Mass Destruction (WMD)/CURVEBALL case, where sharing intelligence and sharing access to the source of the intelligence between Germany's Federal Security Service (BND) and the US Central Intelligence Agency (CIA) - who was not given access, except for one officer - was not made possible as to be expected of allied intelligence services. Next, Clark cites the failure to analyze intelligence on a given issue, especially in a manner irrespective of the current mindset of policymaker or analyst[4]. Clark notes the mindset -

2. Trafton, "Intelligence Failure and Its Prevention", ii.

3. Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press, 2010), 2.

4. Clark, 3.

a set of preconceived notions held by a policymaker or analyst on any given issue - is a common denominator of most intelligence failures.[5] Clark's last major note about the overview of why we fail and, subsequently, why intelligence fails is the failure of the intelligence customer to understand the information the intelligence is conveying, or failure to make an appropriate decision based upon the intelligence received[6]. Clark then discusses briefly how wishful thinking regarding intelligence-policy decisions played a role in the intelligence failure of Soviet Premier Joseph Stalin's response to intelligence regarding Germany's pending Operation Barbarossa[7] - the act of declared war on the Soviet Union.

Robert Jervis, a well-known scholar of intelligence studies, writes that intelligence failure, "is a mismatch between the estimates and what later information reveals to have been true."[8] Jervis notes two major points in his prose and exhaustive footnotes. 1) In many instances, intelligence is frequently incidental in the accuracy of assessments and estimates provided by the reporting, and 2) most of the notice paid to intelligence failures by government and the public were regarding the more dramatic and spectacular failures (i.e. Pearl Harbor and 9/11).[9] It is these such dramatic traumas and the subsequent tragedy of such events that compels government to create new

---

5. Clark, *Intelligence Analysis*, 3.

6. Clark, 4.

7. Clark, 1.

8. Robert Jervis, "Reports, Politics, and Intelligence Failures: The Case of Iraq," *The Journal of Strategic Studies*, 29, no. 1 (February 2006), 10.

[9] Jervis, 10.

legislation to “prevent” future tragedies and spurs the public to side with the government in chastising the IC. While such reactions are understandable (and the resulting new policies may not be), the fact that intelligence is prone to failure may be disconcerting to outsiders whose only frame of reference to intelligence are the James Bond or Jason Bourne film series. Such erroneousness in intelligence is often the norm. After all, intelligence services are managed and operated by humans, and humans are fallible and prone to errors.

Furthering Jervis’s point is a statement made in a recent interview from a 28-year veteran of the CIA National Clandestine Service (now the Directorate of Operations), John Sipher, in which he states, “intelligence collection is not an efficient business; it can be very effective, but it’s not efficient.”[10] Sipher’s comment that intelligence *can* be effective is revealing. His comment implies that intelligence is not always efficient (thus we have failures) and speaks to the inherently ambiguous nature of intelligence and the complexities displayed by the nuance of the information obtained and analyzed within the IC.

The lack of efficiency in a data-driven and often data-overloaded business such as intelligence, and under increasing bureaucratic complexity, is also a contributor to intelligence failure. In the end, intelligence cannot and will not always be correct on any given situational assessment or predictive estimate because intelligence collection and

10. Eddie Mair, “The Eddie Mair Interview*”, BBC Radio 4*, with guest John Sipher, April 4, 2018, Accessed May 5, 2018, https://www.bbc.co.uk/programmes/p063969f (16m:38s-16m:42s).

intelligence analysis are intellectual processes, and processes built upon human intellect are doubtless prone to failure.[11]

Because the normalcy of intelligence failures has slowly become quasi-common knowledge since the time of the Office of Strategic Services (OSS, the precursor to the CIA), the IC does "get it right" from time to time. For example, Mark Lowenthal and Ronald Marks note a report from the Kerr Group, whose members included Richard Kerr (former Deputy Directory of the CIA), Thomas Wolfe, Rebecca Donegan, and Aris Pappas. From their research and analysis, the group concluded that, on the average, "U.S. intelligence called events correctly about three out of four times.[12] But Kerr also concluded that the best way to judge the effectiveness of intelligence analysis was not on a call-by-call basis but by what utility it had for the policymaker. He concluded that the intelligence community did a good job at keeping a very disparate set of policymakers reasonably well informed over 50 years, helping them thread their way through crises and avoid many major crises as well."[13] Lowenthal and Marks go on to say that whatever the record is, whether it is being right 75% of the time or 60% of the time, will have to be as good as it gets.[14] Trying to seek a better percentage of accuracy will incite failure.

---

11. Mark Lowenthal and Ronald Marks, "Is U.S. Intelligence Analysis as Good As It Gets?" *War on the Rocks*, October 23, 2015, https://warontherocks.com/2015/10/is-u-s-intelligence-analysis-as-good-as-it-gets/

12 Lowenthal and Marks, "Is U.S. Intelligence Analysis as Good as It Gets?"

13. Lowenthal and Marks.

14. Lowenthal and Marks.

Despite the record of success over failure as it stands today, the IC will face more failure in the future. Intelligence failure is inevitable, unfortunately. It is unrealistic to expect the IC to not fail on any given intelligence assessment or predictive judgement, and there is a suffering of illusions by those who believe reorganization of the IC will help prevent future intelligence failures or increase the accurate prediction of pending threats. The world today is too dynamic to fit into neat hierarchies; it is too compelling to demand that the IC "connect the dots", as if the world and intelligence are somehow linear in structure; and it is a high bar to set to ask of the IC that the world's events be neatly pieced together in clear, concise warnings of a pending attack. As Richard K. Betts writes, "The available information seldom points unambiguously to the correct conclusion."[15] Accepting the ambiguous nature of intelligence means also accepting that there will be some failure involved.

In reviewing the many definitions and examples of intelligence failure from Trafton, Clark, Jervis, Sipher, and Lowenthal and Marks—all of which have applicability here—and in attempting to illuminate the realistic expectations of what is and is not possible with intelligence, it is helpful to study a historical event of intelligence failure. Not only for the benefit of the historical lessons from the results of a given event, but for the benefit of seeing where intelligence can fail and where intelligence can be effective and succeed at the same time. This will aid in reinforcing the merits of the services intelligence agencies provide to US national security and will help to fully understand and appreciate the limitations of intelligence as revealed by the methodologies and

15. Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), 19.

bureaucracy. Additionally, from these historical failures, we can better pinpoint and bring to common knowledge the realistic expectations intelligence services can provide in bolstering US national security today. Creating a positive understanding of intelligence services - despite their failures and despite the recent trend of democratic governments with nationalist leanings to denigrate intelligence officials and their work in a grotesquely political manner - can help foster a public relations strength that agencies can use to weather the storms of the increasingly polarized modern world.

As one of the "defining interactions"[16] on the geopolitical stage in the long duel between the United States and Russia, espionage has carried much of the popular culture ideas that have been developed regarding the US vs. Russia. Soviet espionage has experienced many ups and downs in its actions and in subsequent successes and failures against the American target. After a period of decline in Soviet espionage operations on the backs of intelligence failures - tracking with the decline and eventual implosion of the Soviet economy and political system - Soviet espionage against the US began to see a resurgence during the 1970s into the 1980s, and through the early 2000s. One example of such resurgence was revealed in 2010 with the Federal Bureau of Investigation's (FBI) Operation Ghost Stories[17] - an intelligence success for the US IC and an intelligence failure for Russia's Illegals program, a hallmark of Russian intelligence operations.

16. Katherine L. Herbig and Martin F. Wiskoff, "Espionage Against the United States by American Citizens 1947-2001" (Monterey, CA: Defense Personnel Security Research Center, 2002), 5.

17. "Operation Ghost Stories: Inside the Russian Spy Case", *Federal Bureau of Investigation*, October 31, 2011, https://www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case

According to a study entitled, “Espionage Against the United States by American Citizens 1947-2001”, the authors Katherine L. Herbig and Martin F. Wiskoff note that during the 1980s - a decade seen by some as a “renaissance” of Russian espionage activity after critical setbacks in their network of foreign contacts during the 1930s-1950s[18] - more than 60 US citizens were arrested for espionage or espionage-related federal crimes.[19] From the Herbig and Wiskoff report, the authors note some of the common denominators which categorized American citizens who had been caught spying for foreign intelligence services. Of the personal attributes, Herbig and Wiksoff’s data analysis show that 93% of American spies from 1947-2001 were male, 84% were of white race/ethnicity, 40% were in the 20 to 29 age group, 39% had attained 12 years’ worth of education (what is referred to as a “high school education”), 57% were married, 95% were of heterosexual preference, 83% were born in the United States, and 44% had some kind of foreign attachment, what Herbig and Wiskoff identify as “close family relatives living abroad, emotional ties to persons such as fiancées or friends who were foreign born, or regular business or professional relationships with persons living overseas.”[20] Additionally, Herbig and Wiskoff noted the types of employment and level of security clearance these American spies were under at the time of their committed or

18. Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present* (Washington, D.C.: Georgetown University Press, 2013), 89.

19. Herbig and Wiskoff, “Espionage Against the United States 1947-2001”, 17-18.

20. Herbig and Wiskoff, 18.

attempted acts of espionage. They note 51% were civilians, 33% were employed in the field of communications/intelligence, and 35% held a Top Secret security clearance.[21]

What Herbig and Wiskoff's report reveals what could lightly be interpreted as guiding indicators of persons likely to commit espionage or to be vulnerable to engage in espionage on behalf of a foreign intelligence service because of a person's character weakness, such as alcoholism, financial troubles, marital strife, or workplace and/or ideological discontent. Of these, financial troubles is the most common indicator of espionage potential, as the resulting behavior motivated by such financial trouble can be observable to both foreign intelligence officers conducting spotting and assessing, and to counterintelligence officers on the lookout for the "insider threat", or mole. Financial problems are viewed as a "trigger", and when combined with other social triggers can be used in identifying those likely to commit espionage.[22]

Many students of intelligence studies will recall the decade of the 1980s as infamous for the number of espionage-related arrests that were made, as well as the year 1985, which the news media had dubbed as the so-called "year of the spy".[23] One of the most infamous espionage cases during this decade was that of Aldrich Hazen Ames, a career CIA intelligence officer, formerly of the Soviet and East European

21. Herbig and Wiskoff, 18.

22. Herbig and Wiskoff, "Espionage Against the United States 1947-2001", 14.

23. Sulick, *American Spies*, 90.

Division[24] (SE Division) and later demoted to counternarcotics,[25] who began spying for the Soviet Union's *Komitet gosudarstvennoy bezopasnosti* (KGB) in 1985. Former CIA officers Sandra Grimes and Jeanne Vertefeuille have authored a detailed account of their time working at the CIA as part of the exclusive counterintelligence group dedicated to finding a mole within the ranks of the CIA beginning in 1985. This was the year of the rapid-fire events concerning losses of multiple intelligence officers and agents due to defections, arrests, convictions, etc., which created the impression at CIA headquarters—especially to those of the CI group searching for a mole—that something had gone wrong.

From Grimes' and Vertefeuille's detailed reporting in their book, based upon their decades of experience working in the CIA (often with Mr. Ames), their investigation began to reveal that Mr. Ames was showing many of the observable triggers listed by Herbig and Wiskoff: trouble with alcohol, financial problems, marital strife (Ames was in the process of divorcing his first wife while living with his second wife), and workplace discontent, due to Mr. Ames' poor employee performance evaluations with lower and lower ratings and eventual demotion from SE Division to counternarcotics. Many of the motivators and observable behaviors Ames was demonstrating over the years were

24. Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed* (Annapolis, MD: Naval Institute Press, 2012), 205.

25. Grimes and Vertefeuille, 206.

ignored or simply not reported up the chain of command within the CIA's Office of Security.[26]

Robert Ames began to meet and assess Soviet embassy employees in the Washington, D.C. metro area for suitability as intelligence recruits. This work was part of a routine task in which he aided a certain CIA office. This provided Ames with the cover he needed to offer his services and begin his espionage against the US. Adding to this, Ames was still employed in counterintelligence (CI) at the CIA. This afforded him great "access to both former and active CIA operational cases involving Soviet intelligence officers."[27] Ames developed a cover identity in which he identified himself to potential intelligence recruits as a Sovietologist. In this cover for more than a year, Ames eventually contacted an incoming Soviet embassy official, Mr. Sergey Dmitriyevich Chuvakhin. Ames then misled his superiors at the CIA, who thought he was meeting with Chuvakhin to assess him as a potential intelligence source, and Mr. Chuvakhin assumed Mr. Ames was meeting him based on engaging in friendly discussion on U.S.-Soviet relations, by way of Ames's "Sovietologist" cover.[28]

In April of 1985, Ames met with Chuvakhin at the Soviet embassy in Washington and without speaking explicitly of what he wanted, left an envelope at the embassy that contained a note describing Ames's wishes to offer information, and offering a few

---

26. Select Committee on Intelligence, United States Senate, "An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence" (Washington: U.S. Government Printing Office, 1994), 4-11.

27. Select Committee on Intelligence, 12.

28. Select Committee on Intelligence, "An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence", 12.

pieces of intelligence that Ames believed would help to establish his own competency as a source; *bona fides* in intelligence parlance.

A month later Chuvakhin summoned Ames to a lunch meeting, after which Ames again went to the Soviet embassy. Once inside, he was informed that his offer to work on behalf of the KGB was approved, along with a payment of $50,000.[29] Because of Ames's increasing financial troubles, this supposed "one-time" payment of such a sum only spurred him to continue to commit espionage on behalf of the Soviet Union. Given Ames's access to intelligence reports, officials, knowledge of active and planned operations, and his work as a CI officer (mediocre as he may have been), it is easy to see why Ames chose to continue to work on behalf of the KGB.

Up until the Ames case, many of the indicators of potential to commit espionage were not readily available on the minds of IC officials. In the 1980s, much of the IC's attention was still devoted to the Soviet and Eastern European targets[30], and for good reason. During that decade, "80 percent of American spies passed their secrets to the Soviet Union and its allies."[31] The Soviet satellite republics were well-trained in taking advantage of a character flaw or vice in recruiting a potential intelligence asset. Ames was easily recruited by money. Ames was one of the few American spies to have earned any substantial sums of money for his espionage efforts. Soon, Ames was living

29. Select Committee on Intelligence, 12-13.

30. Grimes and Vertefeuille*, Circle of Treason*, 95.

31. Sulick, *American Spies*, 91.

beyond his means, buying designer suits, purchasing a Jaguar and paying more than $500,000 in cash for a house[32], all on a supposed government salary.

The intelligence failure here lies in either not reporting the above indicators or simply ignoring them. Following the damaging 1970s era of James Angelton's paranoid mole hunt, which ended with no mole being found, the CIA during Ames's espionage was reluctant to believe there really was a mole in their ranks. This disbelief continued even though SE CI Division was given continued support to conduct a mole hunt. Ames was a walking billboard displaying his outright espionage for a foreign power, and the very agency he worked for and betrayed chose to continue its work in disbelief. Of this, Sulick writes, "If anyone at the CIA had paid a modicum of attention to these indicators, he might have been caught before 1994."[33] Changes made after the Ames case have not prevented the intelligence failure of the classic mole working under our nose. It may have slowed down and given some pushbacks to those attempting to commit espionage, but this kind of intelligence failure will continue.

In 2001 Robert Hanssen of the FBI was arrested on charges of spying for the SVR, successor to the KGB. He was found guilty and sentenced to prison. Hanssen spied for Russia for more than 20 years, and he, too displayed many of the actions and observable behaviors that we now know as indicators of espionage.

Following Ames's arrest and conviction, Congress, in 1995, authorized a bill that required every government agency to provide notice to the FBI in a timely manner on all matters concerning any sign that classified information is suspected to have been given

32. Sulick, 196.

33. Sulick, 196.

to a foreign intelligence service. Again, as we see after 9/11, is a failure to share intelligence. If the CIA has intelligence regarding a mole within its ranks and does not notify the FBI, then no criminal prosecution can occur. Just as intelligence failure will continue to occur, so too will the intelligence failure that is the threat of the mole continue to occur. Such downfalls are inevitable.

For every intelligence failure that comes to light, it will be critical to understanding and security to assess the lessons from the results of a given event. This is not only to the benefit of practitioners and scholars in helping them see where intelligence can fail and where intelligence can succeed, but also to aid in reinforcing the merits of the services intelligence agencies provide to US national security. A growing understanding and appreciation of the limitations of intelligence as revealed by the methodologies and bureaucracy appears to be on the rise. This is good news for intelligence agencies. Additionally, from the lessons we ascertain from historical, recent, and future intelligence failures, we can better pinpoint and bring to common knowledge the realistic expectations intelligence services can provide in bolstering US national security today.

In the whirlwind age of globalization, intelligence agencies will face even more challenges with intelligence failure in the form of espionage. As migrants flee war-torn rogue states and hostile nation-states and settle in democratic countries and elsewhere, allegiances to national identities and alliances will be subject to cross-pollination, creating hybrid allegiances and alliances among citizens. This presents a dilemma to the intelligence community as it will add yet another layer of threat, tying onto the ideology-based espionage threat that has carried over from the days of bipolar

superpowers and is now morphing into the hybrid alliances and allegiances that globalization has brought to many developed countries.

Citizens committing espionage while maintaining a dual patriotic fervor to divergent alliances will present a new kind of espionage threat, according to Herbig and Wiskoff. They write: “How does the nation state, now facing espionage from many quarters, minimize its vulnerability from divided or diluted loyalties if ever more of its citizen come from other nations, maintain foreign attachments, and view life in any particular nation as merely a temporary stay until something better opens up elsewhere around the world?”[34] The imperative here of the intelligence community to adapt to the new espionage threat looms in the face of the swift changes in hybrid alliances and allegiances. “The traditional concept of national intelligence,” Herbig and Wiskoff write, “breaks down in a global economy.”[35]

The pending failure here will be the IC’s inability to adapt to this new style of espionage threat in the face of increasing chaos from globalization. Perhaps this failure will not be as noticeable given how seemingly diffuse the threat is and will not have the public or lawmakers crying out for “intelligence reform!”, but the threat is real and the need for adaptation is real. Finding a way forward for the intelligence community and the national security clearance model will be a critically complex mission in support of US national security objectives.

34. Herbig and Wiskoff, “Espionage Against the United States 1947-2001”, 72.

35. Herbig and Wiskoff, 72.

Bibliography

Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press, 2007.

Clark, Robert M. *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C.: CQ Press, 2010.

Grimes, Sandra and Jeanne Vertefeuille. *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed*. Annapolis, MD: Naval Institute Press, 2012.

Herbig, Katherine L. and Martin F. Wiskoff. "Espionage Against the United States by American Citizens 1947-2001." Monterey, CA: Defense Personnel Security Research Center, 2002.

Jervis, Robert. "Reports, Politics, and Intelligence Failures: The Case of Iraq." *The Journal of Strategic Studies* 29, no. 1 (February 2006).

Lowenthal, Mark and Ronald Marks. "Is U.S. Intelligence Analysis as Good As It Gets?" *War on the Rocks*. October 23, 2015. Available https://warontherocks.com/2015/10/is-u-s-intelligence-analysis-as-good-as-it-gets/

Mair, Eddie. "The Eddie Mair Interview*." BBC Radio 4*. With guest John Sipher. April 4, 2018. Accessed May 5, 2018. Available https://www.bbc.co.uk/programmes/p063969f (16m:38s-16m:42s).

"Operation Ghost Stories: Inside the Russian Spy Case." *Federal Bureau of Investigation*. October 31, 2011. https://www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case

Sulick, Michael J. *American Spies: Espionage Against the United States from the Cold War to the Present*. Washington, D.C.: Georgetown University Press, 2013.

Trafton, Dwight E. "Intelligence Failure and Its Prevention." Naval War College, 1994.