The Politics of Intelligence

Applying History to Modern Day Threat Intelligence

Biography

Paul jaramillo
@DFIR_Janitor

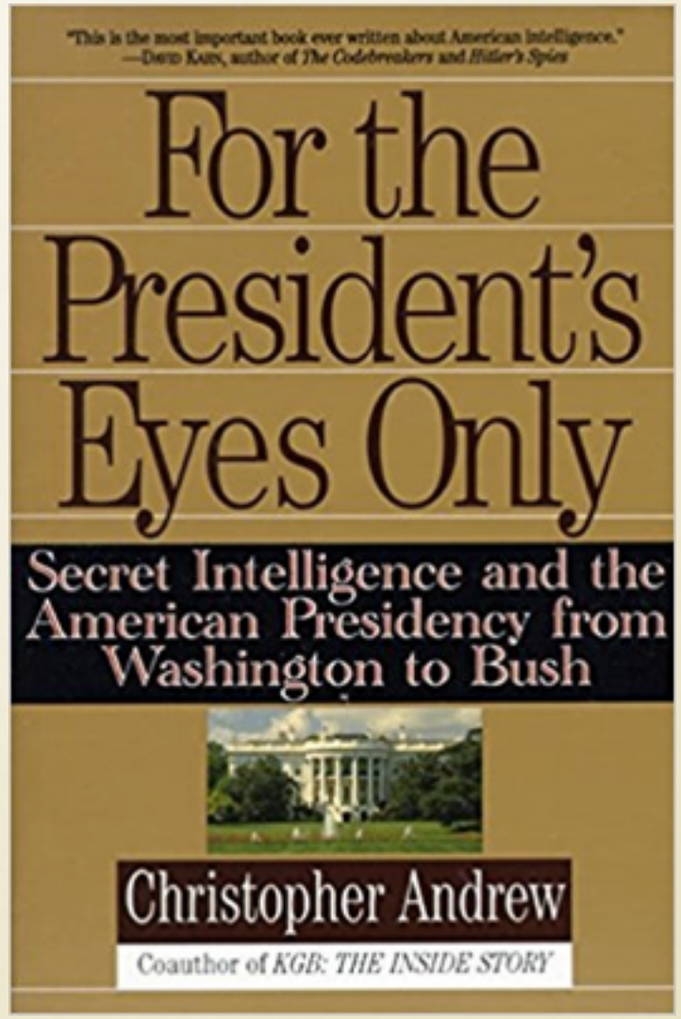
Currently:
Sr. Mgr, DFIR @Splunk

Previously:

- CrowdStrike Services
- Fortune 200 Energy
- Fortune 100 Manufacturing
- Fortune 10 Conglomerate
- Dept. Of Energy
- Fortune 100 Telco

Agenda

- State of Affairs
- Pre-WWII
- Failure of Imagination
- Keeping Up With the Joneses
- It's Over 9000
- Being Milton
- Politicized Intel
- Recommendations

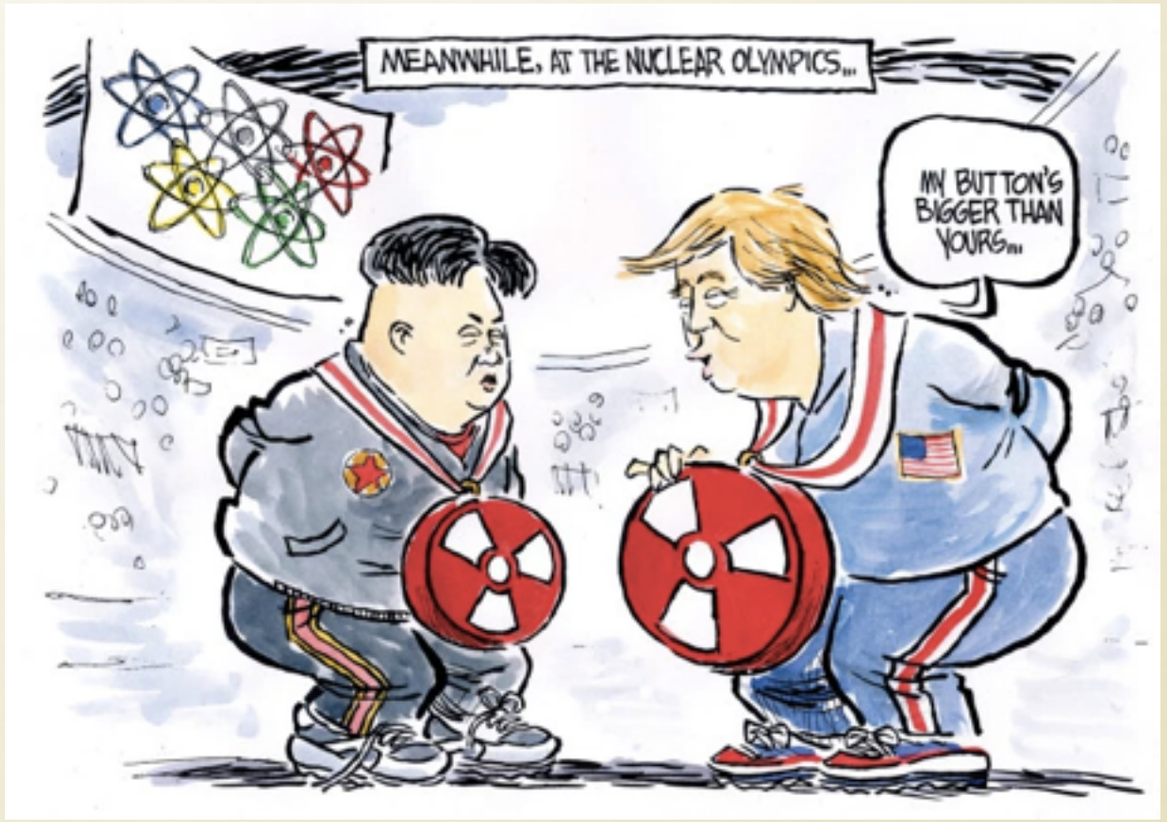


State of Affairs

- **Tactical CTI** = Sinking a 3ft putt (frameworks, less friction, binary, reduced lead time, etc)
- **Strategic CTI** = 300yd drive dead center in the fairway (higher barrier to entry, customer indifference, structured guessing, etc)

State of Affairs

- My feed is yuge!
- Non-operationalized "fusion centers", repackaging not creating new analysis
- Intel analyst hiring misses
- Poor work product



America's 1st Spymaster

"It is by comparing a variety of information, we are frequently enabled to investigate facts, which were so intricate or hidden, that no single clue could have led to the knowledge of them. In this point of view, intelligence becomes interesting which but from its connection and collateral circumstances, would not be important" -GW

- Suffered utter defeat with General Braddock at the hands of the French in 1755, blamed poor intel
- 1775 helped established Committee of Secret Correspondence
- Famous Culper spy ring used invisible ink
- Deception ops inflated his troop totals to prevent British attack
- Deception ops feigned NYC attack so French could land safely
- Used a school teacher to decrypt British dispatches leading to Cornwallis' defeat at Yorktown
- 1790 established Secret Service Fund for Intel Operations, in 3 years this grew to $1m or 12% of Federal budget, by War of 1812 fell to $50k

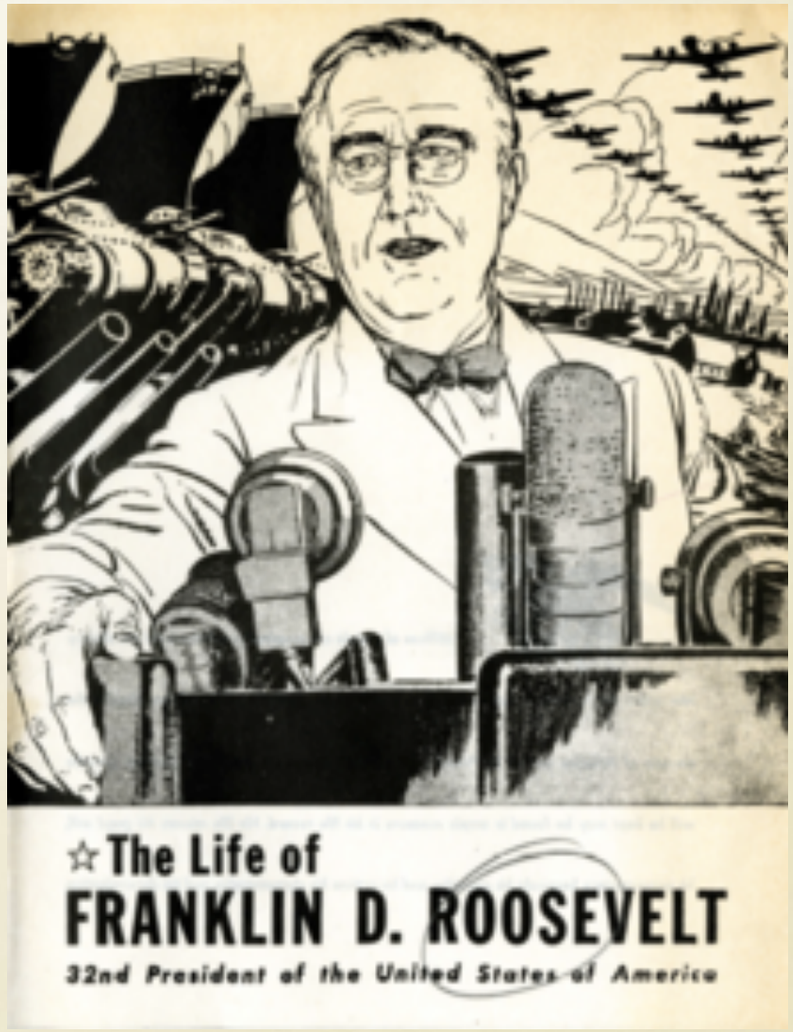
The Isolationist Era

Washington to WWII

- Primarily focus was on military intelligence, with each General having their own spies and also domestic subversion
- "The flight of Abraham" in 1861
- "Sacred 3" codebreakers disrupt Confederates in 1863
- Col. Sharpe's intelligence sways Gettysburg in favor of Federals
- French, Russian, and British("Room 40") codebreakers all had decryption capability of US State Dept. cables
- MythBuster: Lusitania vs Zimmerman Cable
- Woodrow Wilson admitted much to his own surprise and ignorance that every European country had its own foreign intelligence service, which he didn't believe initially
- Formation of BlackChamber in 1919 to 1929, precursor to NSA, lagged behind others
- Of all people, Truman made the first permanent foreign intelligence and SIGINT agencies and the NSC

Failure of Imagination

- Sep 1940 - US Army's SIS broke Japan's Purple code
- May 1941 - decrypts reveal JP is aware of US code breaking
- Nov 1941 - Army did not provide FDR with "Magic"
- Nov 5 - JP officially decides on Pearl attack
- Nov 25 - FDR states in meeting JP will attack on Dec 1
- Nov 26 - Reports JP force has left Shanghai, FDR warns JP envoy he knows force headed south, envoy informs Tokyo
- Nov 27 - decrypts for embassies to destroy machines, codes, etc
- Nov 28 - FDR goes on vacation?!?!
- Nov 28-30 -US Asiatic fleet warned of imminent JP attack
- Dec 1 - decrypts from Tokyo to Berlin stating war is imminent
- Dec 3 - Tokyo to DC embassy, destroy all but 1 code machine
- Dec 6 - intercepts JP's rejection of terms, delivered partially next day
- Dec 7 - Decoding delays, JP informs US after Pearl attack
- JP naval code JN25b introduced Dec 1940, contained mention of Hawaii on Dec 1 other clues in mid-Nov, only 2 - 5 analysts
- Same thing happened again with Vietnam Tet Offensive, predicted by CIA analyst in 1967



Keeping up with the Joneses

- 1879-82 - Navy Gap - US blindsided during War of the Pacific that Chile had more powerful navy, 1818 congress authorizes funds to rebuild navy, 1882 ONI established, 1885 MID established
- 1938 - Air Power Gap - estimated 6500 German planes only had 1700 operational, allied air power was actually greater, FDR asked for 10k planes
- 1955 - Bomber Gap -USAF claimed 600-800 RU bombers was actually less than 200
- 1957-60 - Missile Gap - USAF/NIE estimated 100 to 1500 RU ICBMs vs 130 US, the reality was RU had 4 ICBMs

It's Over 9000

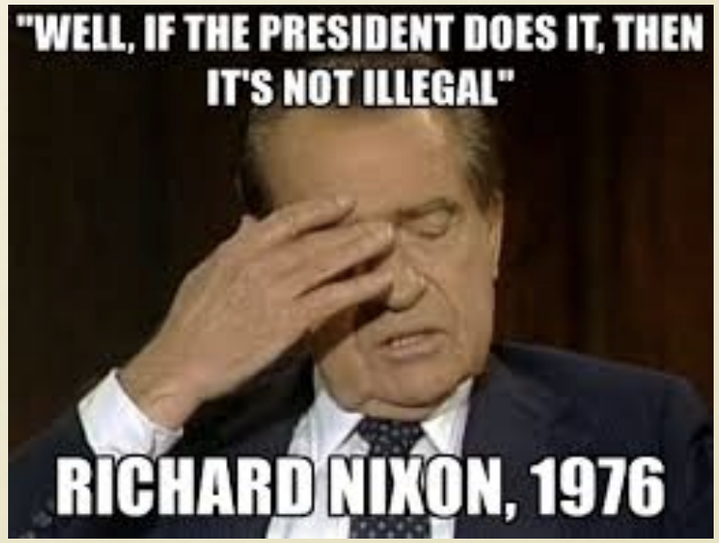
- 1952 DCI Bedell Smith reported 1500 agents in North Korea, the reality was the Seoul office had staff of 200 none of whom spoke fluent Korean, no value ever yielded from HUMINT and DCI was too embarrassed to admit to other branches
- 1961 Dulles stated that Cuban invasion had high chances of success, State was skeptical, even Kennedy had grave doubts, advising Marine had only done 1 combat amphibious landing, 1400 troops vs 20K
- 1977 CIA's first briefing with Carter dazzled him with new cutting edge Keyhole satellite imagery, which despite his distrust of the CIA gave him an inflated view of their capabilities

Being Milton

- FDR was receiving 50 decrypts a day, never directed any action based on SIGINT
- Not until 1946 when Truman raged, did he get a summarized intelligence daily brief
- In 1961, CIA devised the "President's Intelligence Checklist" delivered every morning by an analyst that could answer questions, for the first time report was tailored to JFK's interests and the CIA had an active consumer of intel
- 1963 - 10 days into LBJ's presidency, halted CIA briefings, asked for single page to read before bed, only feedback every was complaint that one time the report went to 2 pages
- 1977 - Carter had to take speed reading classes in order to keep up with the amount of intelligence reports hitting his desk

Politicized Intel

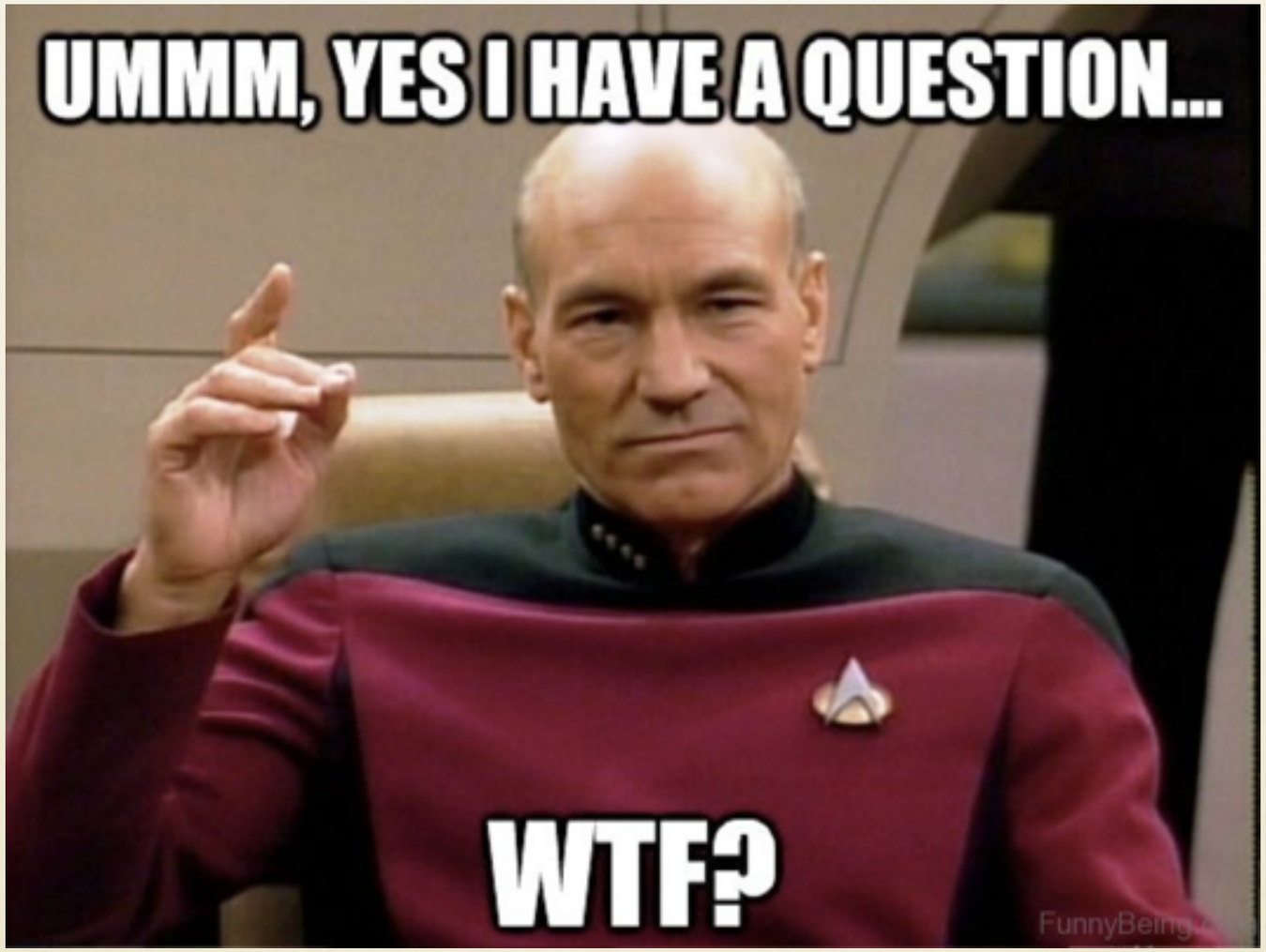
- TR slanted ONI assessments to grow the navy, falsely claimed JP was rebuilding navy, his obsession with battleships caused the US to be painfully short on destroyers
- Gen McArthur didn't believe SIGINT reports of pending CN attacking in Nov 1950 because it didn't fit his narrative
- 1954 Eisenhower commissioned Covert Action Study by his pal Gen. Doolittle, which of course endorsed more covert action
- 1964 to 68 LBJ decides not use the NSC for Vietnam policy but his Tuesday lunch, pushed out people that didn't give him his narrative, led to drastic understatement of enemy troops and ultimately Pentagon Papers



Recommendations

- Failure of Imagination -> Embrace What Ifs & Tackle Unknowns
- Keeping up with the Jones -> Emphasis on peer or competitive intelligence
- It's Over 9000 -> Never Overstate Capabilities
- Being Milton -> Choose Quality over Quantity & Frequency
- Politicized Intel -> Maintain Intellectual Honesty, DCI Helm's example
- Be Like Robert M. Lee!

QUESTIONS?



- Crazy fact: RU stole so many US secrets between 1944-45 they mistakenly started re-using their one-time pads, thus allowing the US to eventually decrypt their cables starting in 1949, which lead to uncovering Fuchs, Cambridge 5, etc