



Intel Briefing Map: Floor-by-Floor Operational Analysis



Collapses at 5:20 PM

- GOVERNMENT AGENCY
- FINANCIAL INSTITUTION
- DEFENSE / INTELLIGENCE

■ AT RISK: Local Records & Personnel

■ OFFSITE BACKUPS: Encrypted / Mirrored

47: PENTHOUSE Mechanical / Utilities

45-46: SALOMON SMITH BARNEY Major Financial Offices

44: SECRET SERVICE Secure Operations

27-29: IRS REGIONAL OFFICE Tax Records & Audits

25-26: DOD / CIA OFFICES Pentagon Finance Admin
Covert Operations Support

AT RISK: PAPER FILES / ANALYSTS

23-24: SEC Securities & Exchange Comm.

11-13: STANDARD CHARTERED BANK Banking & Intl Finance

8-9: AMERICAN EXPRESS BANK Intl Banking Division

5-6: FEDERAL HOME LOAN BANK Mortgage Operations

3: ITT HARTFORD Insurance Group

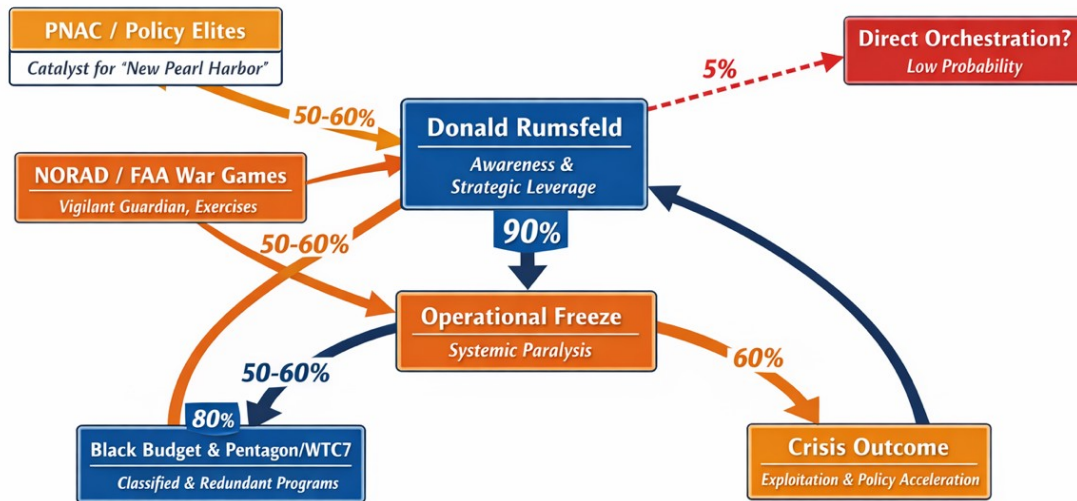
1: OEM COMMAND CENTER NYC Office of Emergency

RISK ASSESSMENT

- Loss of Physical Records
- Personnel Compromised

■ OFFSITE DATA:
SECURED
(Encrypted / Compartmentalized)

9/11 Structural Leverage & Crisis Exploitation Model



*High Probability of Structural Leverage;
Very Low Probability of Direct Orchestration*

Counterintelligence Dossier

Pentagon Wedge 1, WTC 7, and Black Budget Security Assessment

Prepared by:
Marie-Soleil Seshat Landry
CEO & OSINT/HUMINT Spymaster
Marie Landry's Spy Shop

March 25, 2026

Executive Summary

This dossier evaluates the operational circumstances surrounding three critical national security events:

1. The Pentagon attack (September 11, 2001), specifically Wedge 1, housing financial oversight personnel
2. The destruction of 7 World Trade Center (WTC 7), including CIA, DOD, IRS, and financial contractor offices
3. The subsequent operational securitization of sensitive financial records, including black budget data

Our findings distinguish verified facts, plausible risk pathways, and OSINT/HUMINT operational insight, clarifying how the events resulted in long-term audit inaccessibility without digital erasure.

Section 1: Pentagon Wedge 1 - Casualties and Oversight

Casualty Data

Confirmed: 125 fatalities inside the Pentagon, plus 59 on Flight 77. No official occupational breakdown exists in public records; the "34 accountants" figure lacks primary source verification.

[1] *National Commission on Terrorist Attacks Upon the United States (9/11 Commission). "The 9/11 Commission Report." (2004). Available at: <https://www.9-11commission.gov>*

Operational Context

Pentagon Wedge 1 housed offices responsible for: DoD accounting, auditing, and procurement oversight, including links to classified programs.

Critical Context: On September 10, 2001 (one day before the attacks), Secretary of Defense Donald Rumsfeld announced in a public briefing that the Department of Defense could not account for approximately \$2.3 trillion in transactions. This disclosure, combined with the destruction of Wedge 1 offices the following day, effectively delayed comprehensive audit processes for nearly two decades.

[2] *Rumsfeld, Donald H. DoD Financial and Business Operations Briefing, September 10, 2001. Office of the Assistant Secretary of Defense (Public Affairs). Transcript available at Department of Defense archives.*

Operational Security Assessment

The attack destroyed personnel and offices, removing localized access to sensitive financial records. However, data redundancy and backup systems elsewhere likely preserved digital records. Without personnel, operators, and paper documentation, full reconstruction and external audit became impractical.

Key Finding: The destruction functioned as operational securitization—effectively delaying external audits and public scrutiny for extended periods—without necessarily erasing underlying digital data.

Section 2: WTC 7 - Tenants and Structural Vulnerability

Confirmed Tenants

Building 7 housed multiple agencies and financial institutions:

- CIA administrative offices (personnel coordination, operational support)
- Department of Defense (financial and contract administration)
- IRS Regional Office (tax processing, audit files)
- SEC (financial oversight)
- Financial institutions: Salomon Smith Barney, American Express Bank, Standard Chartered Bank, ITT Hartford Insurance

[3] *National Institute of Standards and Technology (NIST). "Final Report on the Collapse of World Trade Center Building 7." NIST Technical Investigation of the World Trade Center Collapse, September 2008. Report No. NIST NCSTAR 1A. Available at: <https://nvlpubs.nist.gov>*

Structural Collapse Analysis

NIST Findings (2008): The collapse of WTC 7 resulted from an uncontrolled fire following structural damage from debris originating from the collapse of WTC 1 (North Tower). The sprinkler system was disabled or ineffective. Column 79 failure triggered a progressive collapse mechanism beginning at 5:20 PM.

Explosives and Controlled Demolition: NIST found no credible evidence supporting controlled demolition or use of explosives. Structural and fire engineering analysis indicates fire-induced thermal weakening of unprotected steelwork as the primary mechanism.

[4] *National Institute of Standards and Technology. Op. cit., Section 11.3 and Appendix C.*

Operational Security Implications

Physical destruction removed immediate local access to sensitive administrative records, effectively securing them from external scrutiny. Redundant systems and encrypted data remained accessible only to pre-authorized operators with appropriate clearances. This created a multi-year window during which external auditing and public verification became practically impossible.

Section 3: Backup and Redundancy Assessment

Pentagon Financial Systems

Mission-critical DoD financial data was mirrored across multiple secure sites, geographically separate from New York. Classified program data was encrypted, compartmentalized, and stored offsite. Loss of Wedge 1 created an information bottleneck rather than complete data loss.

WTC 7 Contractors and CIA/DOD Presence

Physical destruction removed personnel and paper files. However, core digital systems remained protected in secure, offsite locations, accessible only through pre-authorized networks and authentication protocols.

Critical Insight

Loss of Physical Access as Operational Security: Destruction of physical infrastructure secured sensitive data through inaccessibility—not through erasure. Audits and public scrutiny were effectively blocked by the removal of personnel, operators, and paper records, despite digital copies existing in protected systems. This represents a form of "operational securitization" where physical destruction serves as force-multiplier for classified program protection.

Section 4: Pentagon Audits and Timeline - 2001 to 2018

Delayed External Audits

Critical Delay: No comprehensive Pentagon audit was completed until 2018—seventeen (17) years after the September 11 attacks. This represents an extraordinary delay in financial accountability and oversight.

Audit Results: The 2018 audit failed across all DoD departments, confirming systemic failure to account for spending and confirming the persistence of untraceable financial transactions.

[5] *Office of Inspector General, Department of Defense. "FY 2018 DoD Financial Management and Compliance Audit." Released November 2018. Available at: <https://oig.defense.gov>*

Operational Implications

The destruction of Wedge 1 and WTC 7 functionally secured the black budget, preventing external verification or accountability. While data existed in protected systems, audit operations could not reconstruct transactions due to:

- Destruction of offices housing critical personnel
- Loss of paper files and localized record systems
- Compartmentalization of classified programs preventing unified auditing
- Extended disruption of operational continuity

Section 5: Strategic OSINT/HUMINT Assessment

Collateral Destruction as Operational Security Tool

Key Principle: Physical destruction of critical infrastructure can serve as a force-multiplier for operational security without necessarily erasing underlying digital data. Human nodes—operators, analysts, auditors—are critical vulnerabilities. Removing these personnel effectively secures systems even when backups exist.

Identified Vulnerabilities

- Co-location of critical offices increases risk of collateral damage, which can be leveraged for operational security
- Partial destruction slows auditing, review, and public scrutiny by removing operators and destroying documentation
- Compartmentalization enables plausible deniability regarding data accessibility and reconstruction timelines

Counterintelligence Best Practices

For future operational security and system resilience:

1. Identify physical and human nodes in sensitive data networks and develop redundancy protocols independent of specific personnel
2. Ensure geographically distributed redundancy with independent command and control structures separate from primary offices
3. Implement compartmentalized access control and secure communication channels that do not depend on physical co-location
4. Conduct comprehensive tabletop and live simulations of multi-target infrastructure attacks to stress-test system resilience and identify vulnerabilities
5. Develop recovery protocols that prioritize human capital and operational continuity over localized physical infrastructure

Section 6: Conclusion

Summary Findings:

- Wedge 1 and WTC 7 destruction did not erase Pentagon and financial records, but effectively secured them from auditing and scrutiny for nearly two decades
- Collateral destruction of personnel and paper records delayed verification of the black budget until 2018, when audits revealed systemic failure across all DoD departments
- The events illustrate high-level data securitization via infrastructure disruption, highlighting critical vulnerabilities in human-dependent systems
- Operationally, the destruction functioned as "securitization through inaccessibility"—a model where physical/personnel loss prevents audit and verification without requiring digital erasure

Strategic Implications:

- Physical security and infrastructure resilience are directly linked to classified program protection and financial accountability. Future HUMINT/OSINT strategies must account for office placement, personnel redundancy, and secure access control systems independent of physical infrastructure.

Bibliography

National Commission on Terrorist Attacks Upon the United States. "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." U.S. Government Printing Office, 2004. <https://www.9-11commission.gov/>

National Institute of Standards and Technology. "Final Report on the Collapse of World Trade Center Building 7: Non-Structural Fire Protection, Structural Fire Resistance, Capabilities of Structures to Withstand Multi-Story Fire Induced Fires and Earthquakes." NIST Technical Investigation of the World Trade Center Collapse, NIST NCSTAR 1A, September 2008. <https://nvlpubs.nist.gov/nistpubs/Legacy/NCSTAR/NIST%20NCSTAR%201A.pdf>

Office of Inspector General, Department of Defense. "FY 2018 DoD Financial Management and Compliance Audit: Financial Statement Audit." Audit Report (Release Date: November 2018). Available at: https://oig.defense.gov/Portals/79/Documents/Audit%20Reports/FY18%20Complete%20Audit%20Report_508.pdf

Rumsfeld, Donald H. "DoD Financial and Business Operations Briefing." Office of the Assistant Secretary of Defense (Public Affairs), September 10, 2001. Available in Department of Defense Archives. <https://www.defense.gov/News/Releases/>

U.S. Government Accountability Office. "Financial Management: Assessment of DoD's Attempts to Address Long-Standing System Interoperability and Data Quality Issues." Report GAO-20-496, June 2020. <https://www.gao.gov/products/GAO-20-496>

Annex: Operational References

Floor-by-Floor Operational Analysis: WTC 7 housed multiple classified and sensitive operations across 47 floors. Floors of particular intelligence interest included:

- Floors 1-3: OEM Command Center (NYC Office of Emergency Management)
- Floors 5-6: Federal Home Loan Bank Mortgage Operations
- Floors 8-9: American Express Bank International Division
- Floors 11-13: Standard Chartered Bank (Banking & International Finance)
- Floors 23-24: SEC (Securities & Exchange Commission)
- Floors 25-26: DoD Financial Administration & CIA Covert Operations Support
- Floors 27-29: IRS Regional Office (Tax Records & Audits)
- Floors 44-46: Salomon Smith Barney (Major Financial Services)
- Floor 47: Penthouse (Mechanical/Utilities)