Know Your FSB From Your KGB: Researching Soviet/Russian Intelligence in America

David M. Durant
East Carolina University
October 19, 2017

Introduction

- For the past century, Soviet/Russian intelligence has conducted operations within and against the USA
- S/R intelligence activity has on several occasions substantially impacted American history
- New found relevance in last several years

Introduction

- Basic Overview of Soviet Intelligence
- Operations within the US
- Post-Soviet Russian Intelligence/operations within US
- Sources for Research

History of Soviet Security Police (KGB)

- 1917-22: Cheka
- 1922-34: GPU/OGPU
- 1934-1941: NKVD
- 1941;1943-46: NKGB
- 1946-54: MGB
- **1954-91: Committee for State Security (Komitet Gosudarstvennoy Bezopasnosti: KGB)**

KGB Foreign Intelligence

- 1920: INO (International Department)
- 1953: First Main Directorate (FMD) of MGB/KGB

The “Neighbors”: The GRU

- Soviet/Russian military intelligence

- Main Intelligence Directorate of the General Staff

- De facto subordinated to KGB from 1930s-1991

KGB Foreign Intelligence Methods

- Espionage: collecting information from foreign adversaries through human and technical means (spying)
  - Legal and Illegal
- “Active Measures”

"Legal"Espionage

- Legal: run by KGB officers operating under official cover (diplomat, journalist, etc)
- *Rezidentura*: Housed in Soviet diplomatic facility in host nation
- Led by *Rezident:* senior KGB officer

Illegals

- Run by Directorate S of FMD
- Operating illegally in host nation, under false identity
- Gather intelligence
- Scout for agents/run agents
- Sabotage in case of war (“break glass in case of emergency”)

The KGB in America

- 1940-1945 was golden age of KGB in USA
- App. 500 Americans tied to CPUSA spied for USSR in 1930s-1940s
- Network led by Jacob Golos/Elizabeth Bentley
- Penetrated State/Treasury/White House/OSS
- Rosenberg cell stole scientific and technical info (including on atomic bomb)

The KGB in America

- Key agents included:
  - Harry Dexter White (Treasury)
  - Alger Hiss (State: GRU)
  - Lauchlin Currie (White House)
  - Laurence Duggan (State)
- Other agents:
  - Rep. Samuel Dickstein (D-NY)
  - Mary Wolfe Price

The KGB in America

- 1945: USA designated as KGB's Main Enemy/Main Adversary (remained so until 1991)

- 1945: KGB espionage efforts in America fell apart
  - Gouzenko defection in Canada
  - Elizabeth Bentley defects to FBI
  - Venona intercepts (1943-46)

- KGB forced to break contact with most of their agents

1948: Washington's Summer of Spies

- July-August 1948: Whittaker Chambers and Elizabeth Bentley testify before HUAC about Soviet/CPUSA espionage
- Hearings/charges become a bitter source of partisan contention
- Charges largely vindicated by archival revelations

The KGB in America

- “Spy mania” caused by HUAC revelations/Rosenberg trial helped foster rise of McCarthyism/”Red Scare”
- Source of bitter partisan divisions
- Scientific/technical secrets obtained by KGB helped USSR catch up militarily
  - Atomic bomb in 1949
  - Radar/proximity fuses aided communist effort in Korea

The KGB in America

- From 1950s through 1980s, KGB forced to rely on traditional inducements ($) to recruit American spies
- Ideological recruits mostly anti-American, not pro-Soviet
- Legal Rezidentura in Washington, New York, and San Francisco

The KGB in America

- Key agents include:
  - John Walker, Jr. (Navy: 1967-85)
  - Aldrich Ames (CIA: 1985-94)
  - Robert Hanssen (FBI: 1979-2001)
  - Christopher Boyce/Andrew Daulton Lee (TRW: 1975-76)

Active Measures

- Use of propaganda and disinformation to advance USSR interests, undermine adversaries
- Provocations/false and misleading information/“Fake news” stories/forgeries/
- Influence target audience (public and decision makers)

Active Measures in America

- Intended to foster and exploit division in US society
- Increase anti-Americanism abroad
- More successful overseas than in USA

Active Measures in America

- Anti-USA active measures campaigns:
  - JFK conspiracies
  - Quebec CIA forgeries
  - Philip Agee
  - AIDS
  - Baby parts
- Prompted effective US response in 1980s

The KGB in America

- Much of the KGB felt they were winning the struggle against the “Main Enemy” up until the Soviet collapse

Russian Intelligence Today

- KGB broken up into several parts in 1991
- Most internal security functions became part of Federal Security Service (FSB)
- First Main Directorate became

Foreign Intelligence Service (SVR)

- GRU gained autonomy

Russian Intelligence Today

- Russian Intelligence Services (RIS) see themselves as successors to Soviet security services

- Fundamental continuity of methods and worldview (adapted for digital age)

Russian Intelligence Today

- America is still the “main target”
- RIS see themselves at war with USA/liberal West (M. Galeotti)
- Belief that USSR was subverted by USA/West
- Fear that this will happen to Russia via “color revolutions”/democracy promotion
- RIS seek to weaken and discredit USA/NATO/EU

Russian Intelligence Today

- *"Listen: we engage in foreign policy the way we engage in war, with every means, every weapon, every drop of blood. But like in war, we depend on both the strategy of the general in the High Command, and the bravery and initiative of the soldier in the trench."*

- Former Russian diplomat to Mark Galeotti, April 2017

Source: Controlling Chaos: How Russia manages its political war in Europe (http://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe)

Russian Intelligence Today

- RIS compete against each other to carry out broader agenda (FSB v. SVR v. GRU)
- RIS Environment encourages aggressive risk taking
- Use of organized crime/financial corruption
- Exploitation of digital/cyber capabilities
- Soviet-era methods updated for 21st century

Espionage: Traditional and Cyber

- Continued human espionage: legal and illegal
- Use of hacking to supplement human espionage
- RIS are believed involved with several of the most sophisticated hacking operations today
  - APT 28: “Fancy Bear (GRU)
  - APT 29: “Cozy Bear” (FSB)
- Digital environment allows better integration of espionage and active measures

Active Measures in the Digital Age

- Russian state media (RT/Sputnik/)
- Cutouts/fronts (Wikileaks)
- Social media trolls/bots (Facebook, Twitter)
- Denial of Service (DDOS) attacks (Estonia, Georgia)

The 2016 Election Hacks

- 2015: Democratic National Committee (DNC) hacked by Cozy Bear (FSB)
- March 2016: DNC and others affiliated with Clinton campaign hacked by Fancy Bear (GRU)
- June 2016: hacked emails released via “Guccifer 2”, “DC Leaks”, and Wikileaks
- Use of “trolls” and “bots” to amplify message

2016 Election Hacks

- *"The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. We assess that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.*

- *We assess with high confidence that the GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks."*

Source: Assessing Russian Activities and Intentions in Recent US Elections. Office of the Director of National intelligence, January 6, 2017. (https://www.dni.gov/files/documents/ICA_2017_01.pdf)

2016 Election Hacks

- *"Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.*

- *We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments."*

Source: Assessing Russian Activities and Intentions in Recent US Elections. Office of the Director of National intelligence, January 6, 2017. (https://www.dni.gov/files/documents/ICA_2017_01.pdf)

The 2016 Election Hacks

- Creation of fake social media accounts to exacerbate existing divisions in US society (left and right)
  - “Secured Borders”
  - “Blacktivists”
  - “LGBT United”
  - “Heart of Texas”
- Attempts to hack state election systems
- No evidence that vote tallies were impacted

The 2016 Election Hacks

- With ongoing US-Russia tensions, and Mueller investigation, topic of RIS activities in America will continue to be in the news, possess cultural resonance, part of partisan political debate

- Important that we as librarians be able to help users find credible sources on this topic

Sources on RIS Activity in USA

- Historical vs. Current

- Great variety of available sources:
  - Federal government information*
  - Web resources*
  - Books
  - Journal articles
  - News articles

Federal Information Sources on RIS Activity in USA

- Congressional
- Executive Branch

Congressional Sources on RIS Activity in USA

- Committee publications (hearings, reports, prints)

- Historical (1934-77):
  - House Un-American Activities Committee (Y4.Un 1/2)
  - House Committee on Internal Security (Y4.UN 8/15)
  - Senate Subcommittee on Internal Security (Y4.J89/2)

- Current (1970s-present):
  - House Permanent Select Committee on Intelligence (Y4. IN 8/18)
  - Senate Select Committee on Intelligence (Y4.IN 8/19)
  - Commission on Security and Cooperation in Europe (Y4. SE 2)
  - House Homeland Security Subcommittee on Counterterrorism and Intelligence (Y4.H 75)

Executive Branch Sources on RIS Activity in USA

- Intelligence Agencies:
  - FBI (J 1.14)
  - CIA (PREX 3)
  - NSA (D 1.2)
  - Office of the Director of National Intelligence (PREX 28)

- FOIA Libraries:
  - https://vault.fbi.gov/
  - https://www.cia.gov/library/readingroom/
  - https://www.nsa.gov/news-features/declassified-documents/
  - https://www.odni.gov/index.php/read-released-records

VENONA

- 2,900 KGB cables intercepted and decoded by Army SIS during the 1940s, declassified in 1995
- Supplemented by Vassiliev notebooks
- Helped answer lingering questions about Soviet/CPUSA espionage

VENONA

National Security Agency: VENONA

https://www.nsa.gov/news-features/declassified-documents/venona/

Federal Bureau of Investigation: VENONA

http://vault.fbi.gov/Venona

Cold War International History Project: Venona Project and Vassiliev Notebooks Index and Concordance

http://www.wilsoncenter.org/article/venona-project

Federal Information Sources on RIS Activity in USA

- GPO Catalog: https://catalog.gpo.gov/
- FDsys: https://www.gpo.gov/fdsys/

Useful Web Resources on RIS Activity in USA: Historical

- Cold War International History Project: https://www.wilsoncenter.org/program/cold-war-international-history-project
- International Spy Museum: https://www.spymuseum.org/
- John Earl Haynes: Historical Writings: http://www.johnearlhaynes.org/
- Through Russian Eyes: https://throughrussianeyes.com

Useful Web Resources on RIS Activity in USA: Current

- Agentura.ru: http://www.agentura.ru/english/
- Chatham House: Russia: https://www.chathamhouse.org/research/regions/russia-and-eurasia/russia
- Marshall Fund: Alliance for Securing Democracy: http://securingdemocracy.gmfus.org/
- In Moscow's Shadow: https://inmoscowsshadows.wordpress.com/
- The Cipher Brief: https://www.thecipherbrief.com/

CWIS Blog & LibGuide

- Blog: http://blog.ecu.edu/sites/cwis/
- LibGuide: http://libguides.ecu.edu/cwis
- Slides and extensive bibliography will be posted to blog

Contact info:

David M. Durant
J.Y. Joyner Library
East Carolina University
Greenville, NC 27858
Ph. (252) 328-2258
E-mail: durantd@ecu.edu