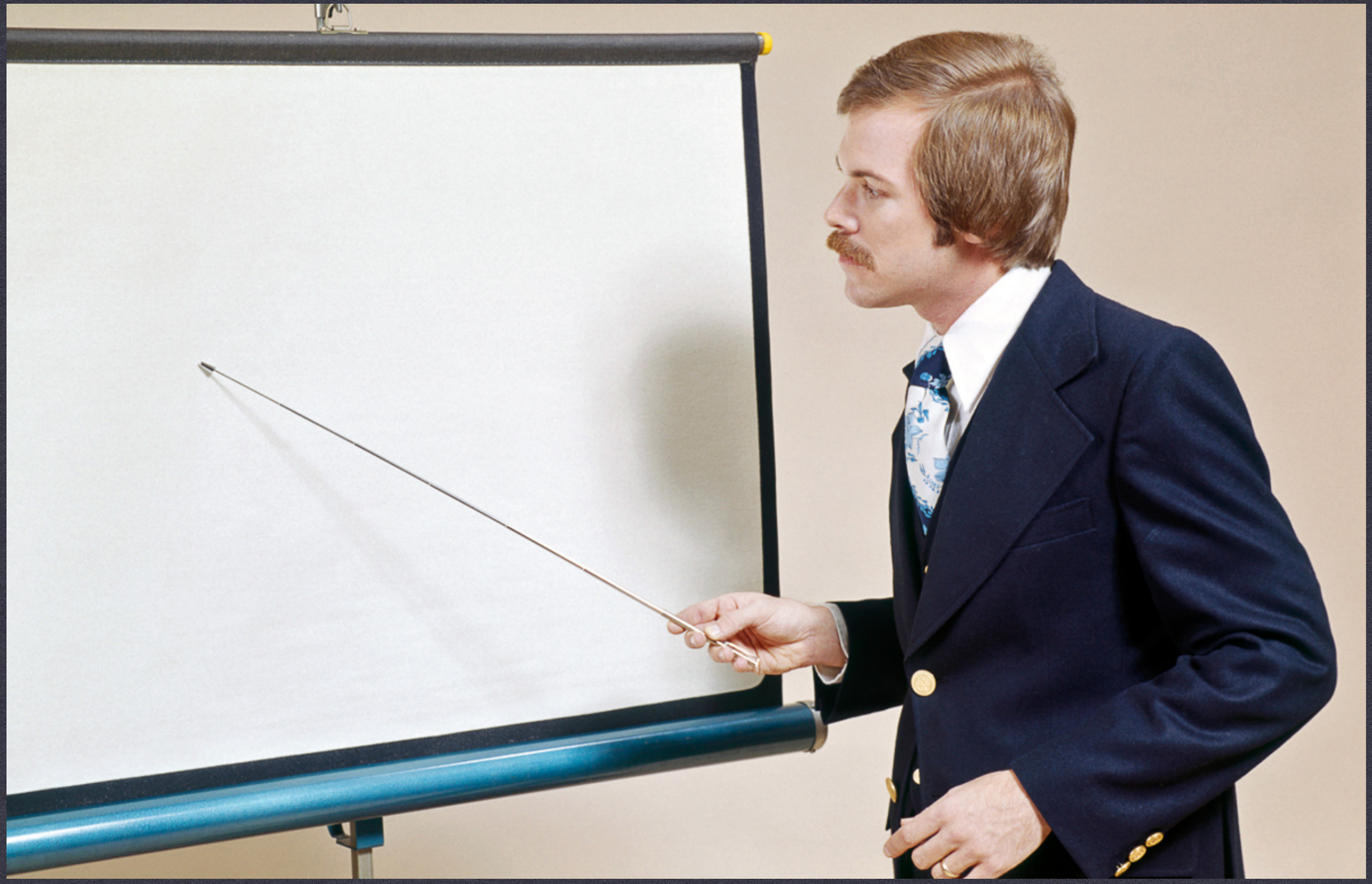
SURPRISE, BITCHES!

ENTERPRISE SECURITY LESSONS FROM TERRORISTS

TROOPERS | THE GRUGQ

- me on twitter: “I’d like to do a talk about terrorist org security for business, ‘dealing with snitches, the insider threat’”
- Enno: “Ok. Your slot is on day 2.”
- me: “it was a joke.”
- Enno: “Too late.”
  - (Famous German sense of humor!)



WHEN IN DOUBT, IT'S A TOUT

DEALING WITH THE INSIDER THREAT

THIS IS NOT THAT TALK…

SORRY.

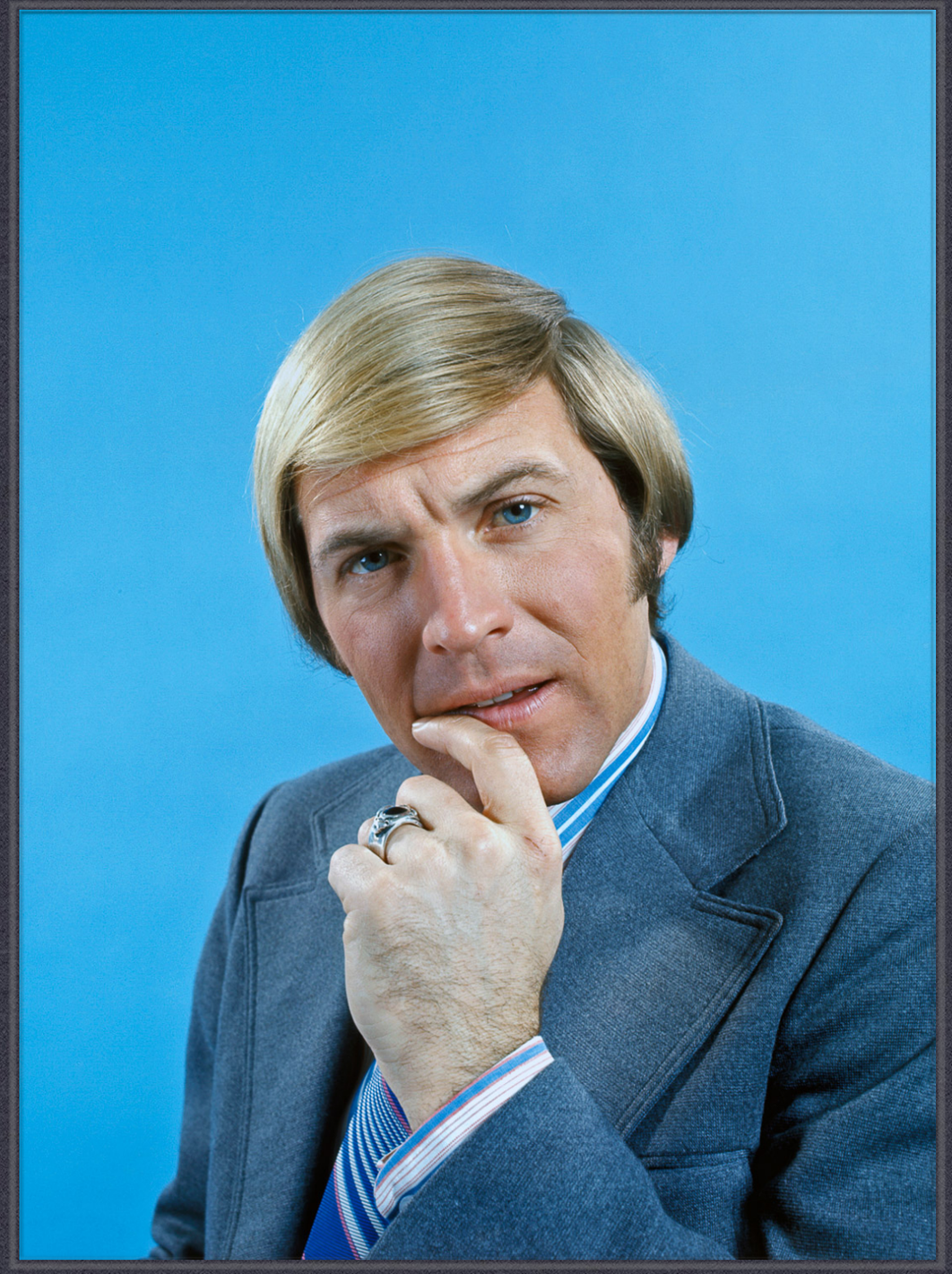
HOW VERY APT

THE GRUGQ (@THEGRUGQ)

Overview

- Intelligence Cycle
- HOWTO: APT
- Cyber Intelligence
- Elements of APT Style
- Conclusion

INTELLIGENCE CYCLE



Intelligence cycle

- Tasking
- Collection
- Analysis
- Dissemination

Tasking

- Customers have a request
  - Customers: policy makers, military, etc
- Request converted into actionable activities
  - What information would address this?
  - Where is it?
  - How do we get it?

Request Deconstruction

- Attempt to answer questions such as:
  - What are the ${*RANDOs*} **capabilities**?
  - What is their **intent**?
  - Do they, or will they, have the **opportunity**?

Collection

- Input -> request for specific information
- Information to resolve the request is acquired
  - Multiple methods and techniques
- Output -> raw intel data for analysis

Techniques

- OSINT: Open Source Intelligence
- HUMINT: Human Intelligence
- SIGINT: Signals Intelligence
- IMGINT: Image Intelligence (planes, satellites)
- Many more…
  - MASINT: Measurement and Signature Intelligence

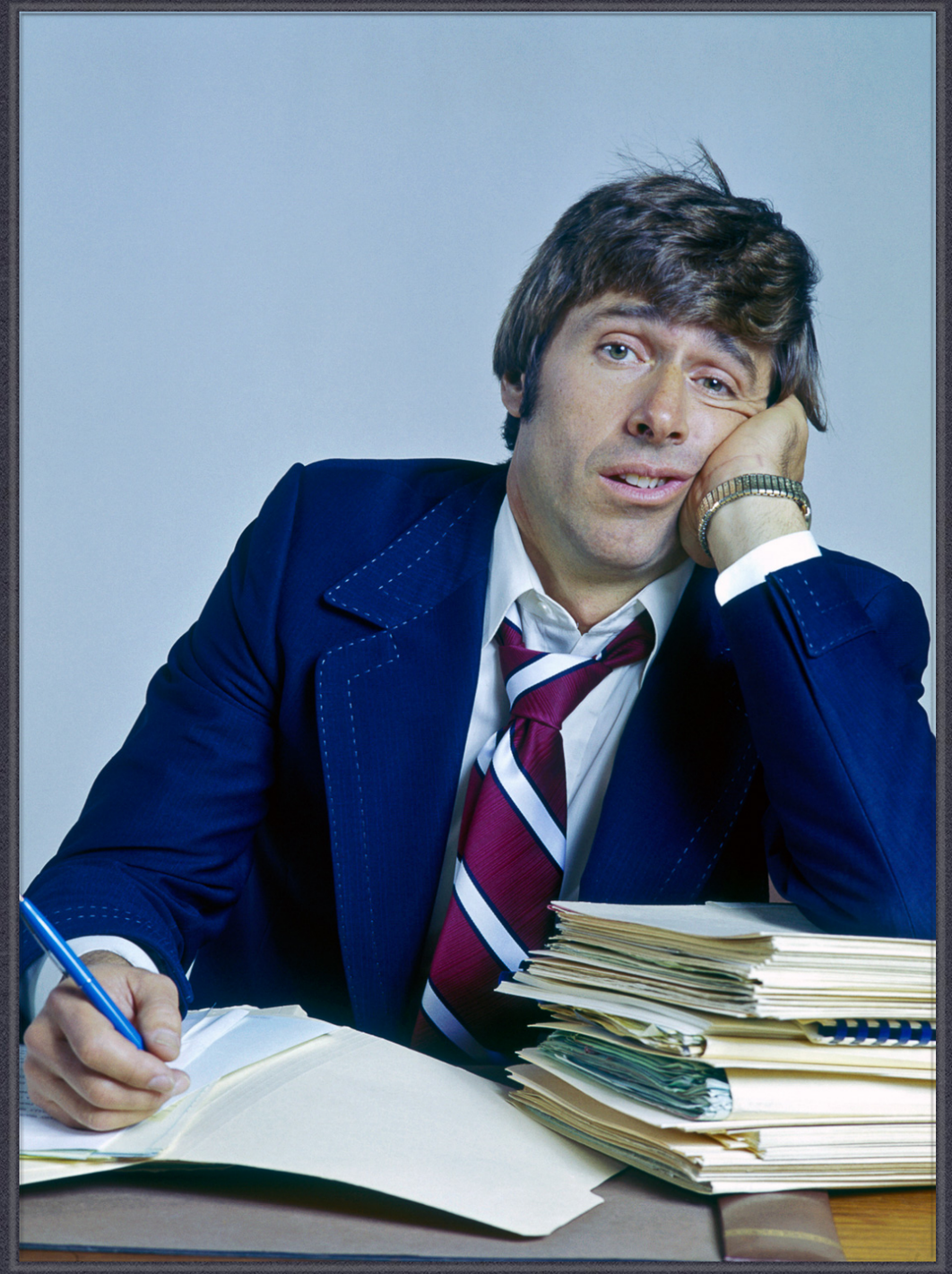
Analysis

- Input -> Raw Data
  - Sift data: is it plausible? authentic? valid?
  - Combine multiple data sources:
    - HUMINT + SIGINT
- Output -> Product

Dissemination

- Input -> Product
  - Distribution filtered by e.g. classification/SCI
- Output -> Policy (in theory)
- Output -> Active Measures

HOWTO: APT



Elements

- Penetration
- Infrastructure
- Analysis
- Management

Penetration

- Hacking tools
  - Recon
  - Exploits
  - Implants
- Developers
- Operators

Tools of the Trade

- Research and Development
  - New tools & techniques
  - Replace/refresh tools lost to attrition
- Maintenance
  - Keep existing tools operational vs evolving defenses
- Training
  - Hackers, developers, and operators

Internal Infrastructure

- Operational
  - Password cracking, fuzzing, etc
- Functional
  - Source repos, comms, workstations, etc

External Infrastructure

- Supporting elements for offensive ops
- Phishing
  - Servers, domains, email setup
- Implants
  - Dump sites, C&C, payload servers
- Everything
  - Staging servers, relays/bounces, post-op cleanup

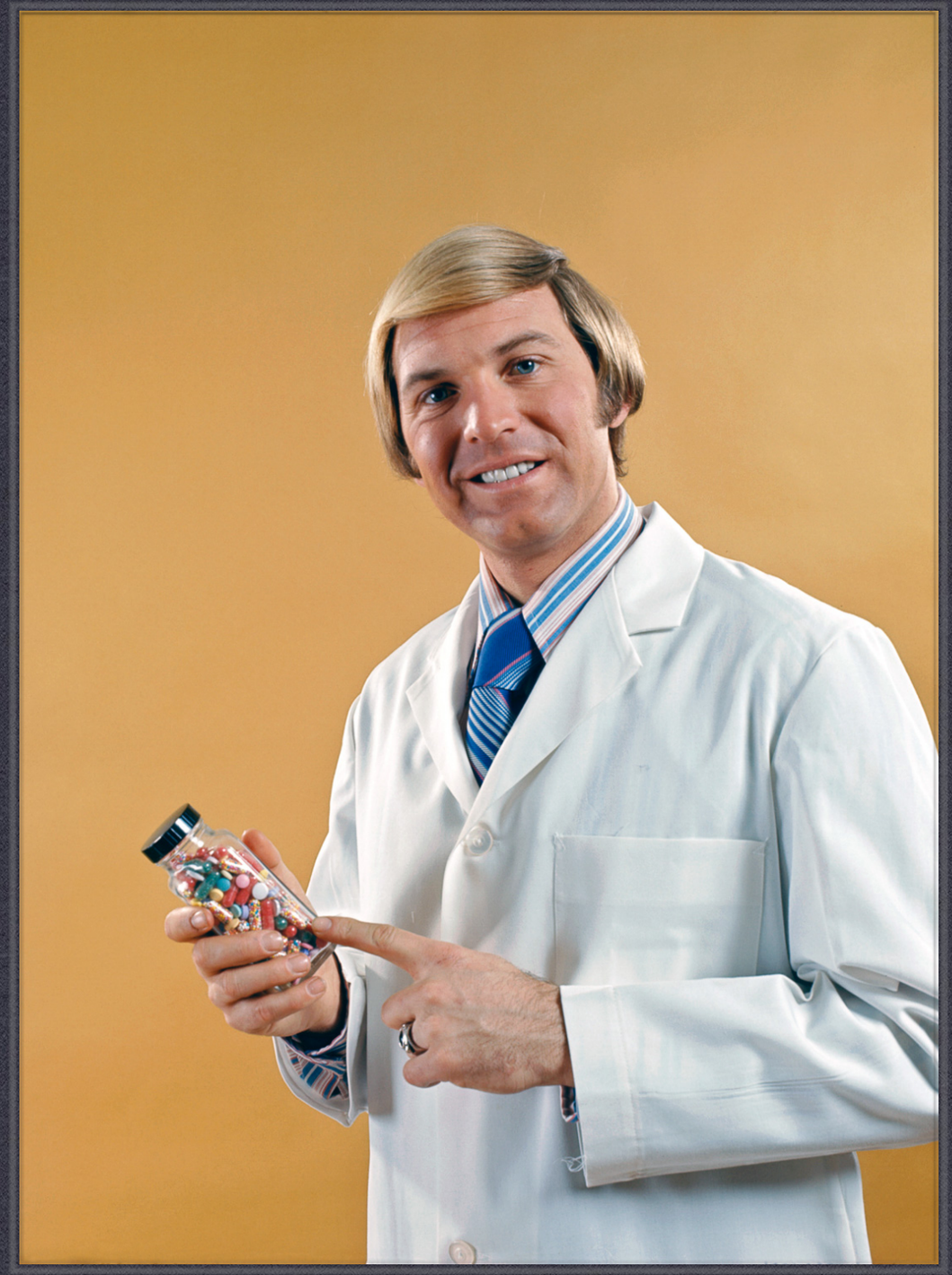
Analysis

- Build an internal “Google”
  - Big data => big problem (terabytes per org)
- Translation
  - Espionage means unlikely the data is “Local”
- Process, Sort, Search, Curate => produce
  - Data is meaningless without context

Management

- Operations
  - Targeting, op design, feedback to Development
- Development
  - R&D, handle feedback/requests from Operations,
- Analysis
  - Tasking, processing, feedback to Operations group
- Top Level
  - Prioritisation, lessons learned, interact w/ customers

CYBER INTELLIGENCE



EVERYONE

THE WAY OF CYBER

- Everyone mixes public/private resources
  - Private firms provide tools, infrastructure, support
    - USA, Russia, China, everyone
- Public sector does operations (typically)

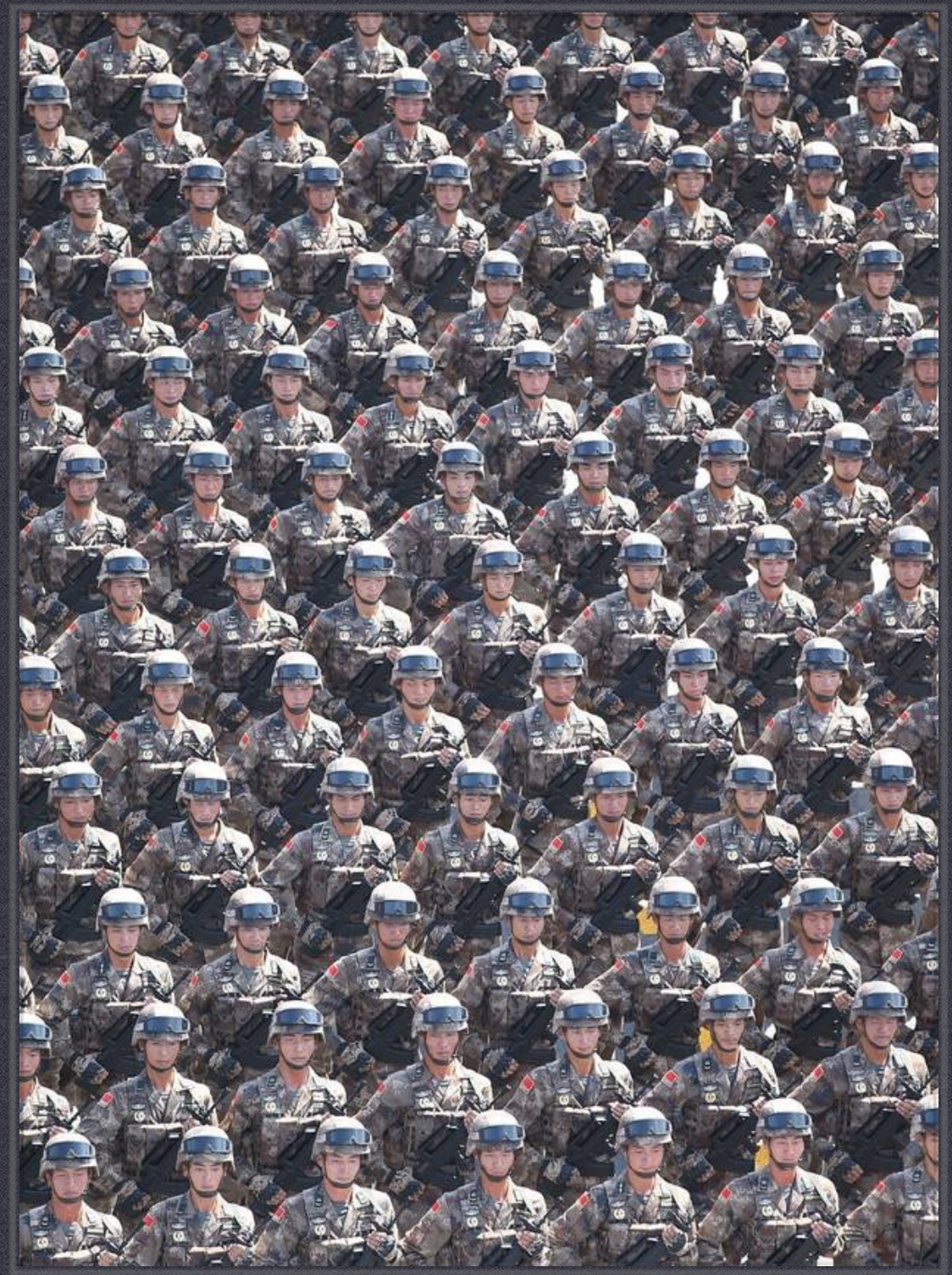
- Command and Control
  - Tight or Loose?
- Ghosting (Covertness)
- Cyber
  - High skill or Low skill
    - (Everyone is a mix, but how much?)

ELEMENTS OF ART STYLE

- Cyber competency
  - How good is their cyber?
    - Can they hack
- Command & Control
  - How tight is the executive & intelligence c2
- Covertness
  - Stealth, how much do they care?

CHINA

THE WAY OF CYBER



- Cyber competency: tiered
- Command & Control: loose
- Covertness: tiered… *cough*

Chinese Way of Cyber

- Tasking
  - Very loose directives from executive
  - Fusion centers for public/private collab.
- Collection
  - Public (3PLA) or private boutique

Chinese Way of Cyber (economic)

- Loose tasking from executive
- Fusion centers for public/private collaboration
  - Private sector helps w/ targeting
  - Fusion centers allow “washing” data back into the private sector
- Collect it all
  - Jiang Tong (tech), SISU (language) both 3PLA feeder schools

Chinese Way of Cyber

- Highly skilled teams
  - Other teams… *cough*
- Political espionage
  - Tibetan diaspora, Uighurs, etc.
- Not obsessed with ghosting

AMERICA

THE WAY OF CYBER

- Cyber competency: tiered (more medium)
- Command & Control: medium
- Covertness: high as fuck

- Tasking from customers is direct(ish)
- Espionage as a tool for “preventing surprise”
  - Spotty track record
- Huge community (1mm “cleared”; 17 agencies; domestic/international division)
  - Huge budget, capability

- Obsessed with Ghosting
- Assume edge case (“hard target”) -> req. 0day
  - Build everything for edge cases
  - Result: everything is expensive, covertness critical, high classification (feedback loop)
- “Contractor Rot”
  - Booze, Raytheon, etc.

RUSSIA

THE WAY OF CYBER

- Cyber competency: tiered (lots of low)
- Command & Control: loose
- Covertness: YOLO

- Loose control
  - Multiple IC components, all competing
- Strategic cyber reserve
  - Complex mix of public and private entities
- YOLOPSEC
  - Not obsessed with ghosting
    - “Fuck you, I’m in Russia, bitch”

- The Covenant
  - Inside the tent pissing out
  - Tools only are OK
- Institutionalized corruption leads to bad things
  - Hackers are coerced to working for individuals
- The gardener and the tool shop… a parable
  - 2015: burned 12 0day; 2016: burned 24 0day
- Flexible, aggressive, uses the strategic cyber reserve, sloppy

“The rocket goes up, it lands in the swamp

That’s how you pay us, that’s how we work”

–Russian Saying

PASSIVE CYBER

- Collection of metadata
- US has a network position advantage
  - Leads to MITM based attacks
- Useful to “know the world”
  - Less useful to “change the world”

ACTIVE CYBER

- Active Measures
  - Requires most of the intelligence cycle
    - Accuracy of output/product is less relevant

CONCLUSION

- Operational characteristics are the result of organizational factors
  - These are historical
  - Different APT groups operate on multiple matrixes of cyber competency, covertness, command & control

QUESTIONS?

THANK YOU.