ASSIGNMENT #7 FINAL PROJECT PRESENTATION

KATY M. WARREN

PROBLEM TO ADDRESS

- The Department of Defense's approach to cyber security has been criticized as lagging behind industry and markedly slow to adapt to new requirements. Understanding the relationship between the current state of the US Cyber Command and industry standards will assist in properly addressing these concerns.

INITIAL RESEARCH QUESTIONS

- What are the trends, themes, and topics of DOD cybersecurity policy since the induction of US Cyber Command?

- To what extent are industry standards represented by DOD Cyber Command policy? To what extent are industry standards **not** represented by DOD Cyber Command policy?

LITERATURE

- Overall, the literature shows a clear and distinguishable divide between the "Dot Mil" cybersecurity culture and network administrators and their private industry counterparts. Calls for greater integration from the Pentagon and independent sources, as well as, proposed initiatives to bridge the divide support claims of policy discrepancies between the defense and the private sectors.

DATA SET: DOD

- The Department of Defense portion of the Policy Balance Dataset was collected from the following online libraries
  - Joint Chiefs of Staff- Doctrinal Publications
    - https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/
    - https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/6-0-Communications-Series/
  - Department of Defense Chief Information Officer
    - https://dodcio.defense.gov/Library/
  - US Cyber Command
    - https://www.cybercom.mil

DATA SET: INDUSTRY

- The Industry portion of the Policy Balance Dataset was collected from the following online libraries
  - NIST Special Publications Library
    - https://nvlpubs.nist.gov/nistpubs/SpecialPublications
  - NERC Resources
    - https://www.nerc.com/pa/comp/Resources/ResourcesDL/Cyber_Security_Standards_Transition_Guidance.pdf#search=cyber%20security
    - https://www.nerc.com/news/testimony/Testimony%20and%20Speeches/Cyber_Security_and_the_Grid_-_Senate_17JUL12.pdf#search=cybersecurity%20standard
  - Mitre Common Vulnerabilities and Exposures
    - http://cve.mitre.org/data/downloads/index.html

POLICY BALANCE SIZE AND AVAILABILITY

- 25 DOD text documents ranging from 2-200 pages. Most between 40 or 50 pages.

- 15 Industry text documents, most between 2 and 20 pages.
  - Risk Management Conference Program 185 pages
  - Common Vulnerabilities & Exposures list 146,000+ data points (.CSV)

- All documents and data files are publicly available.

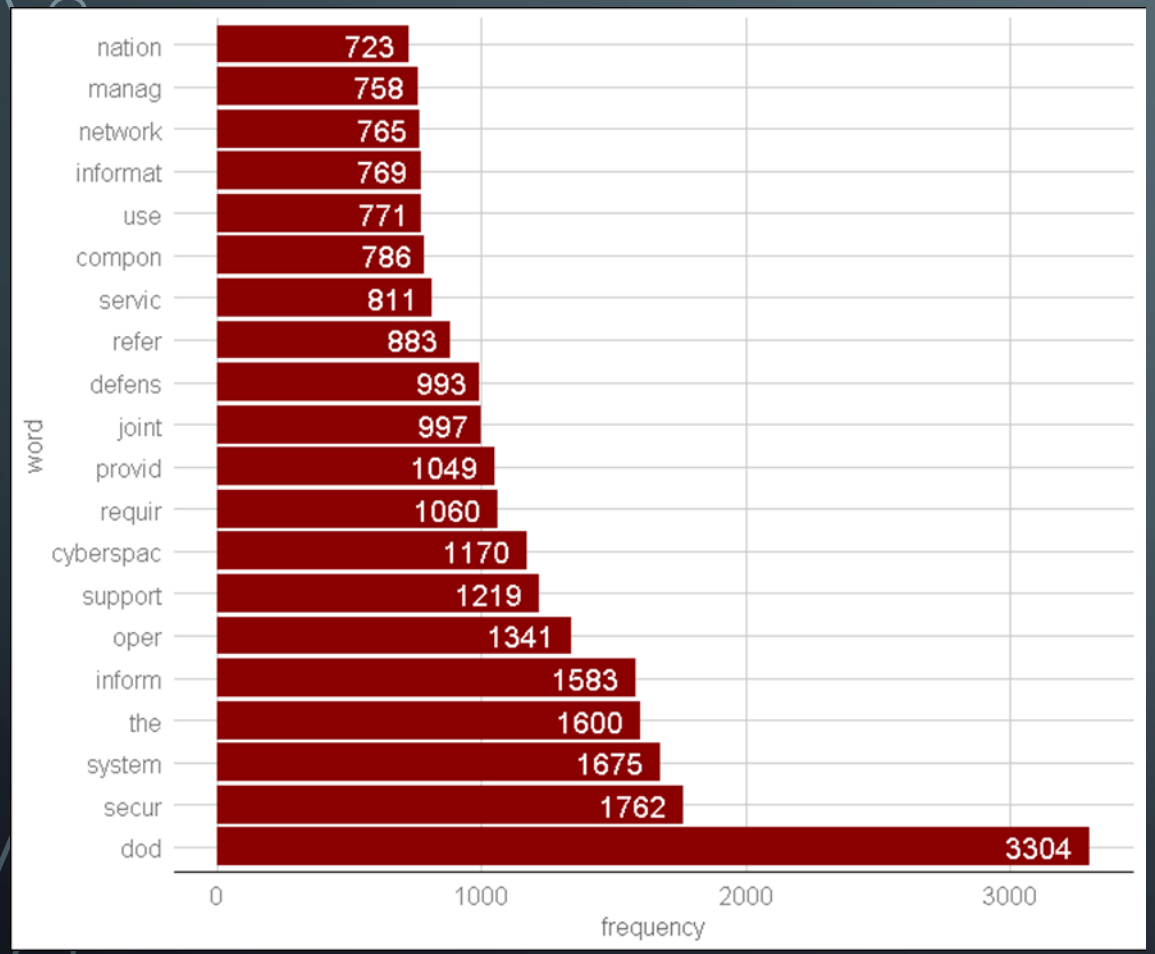
DATA PREPARATION

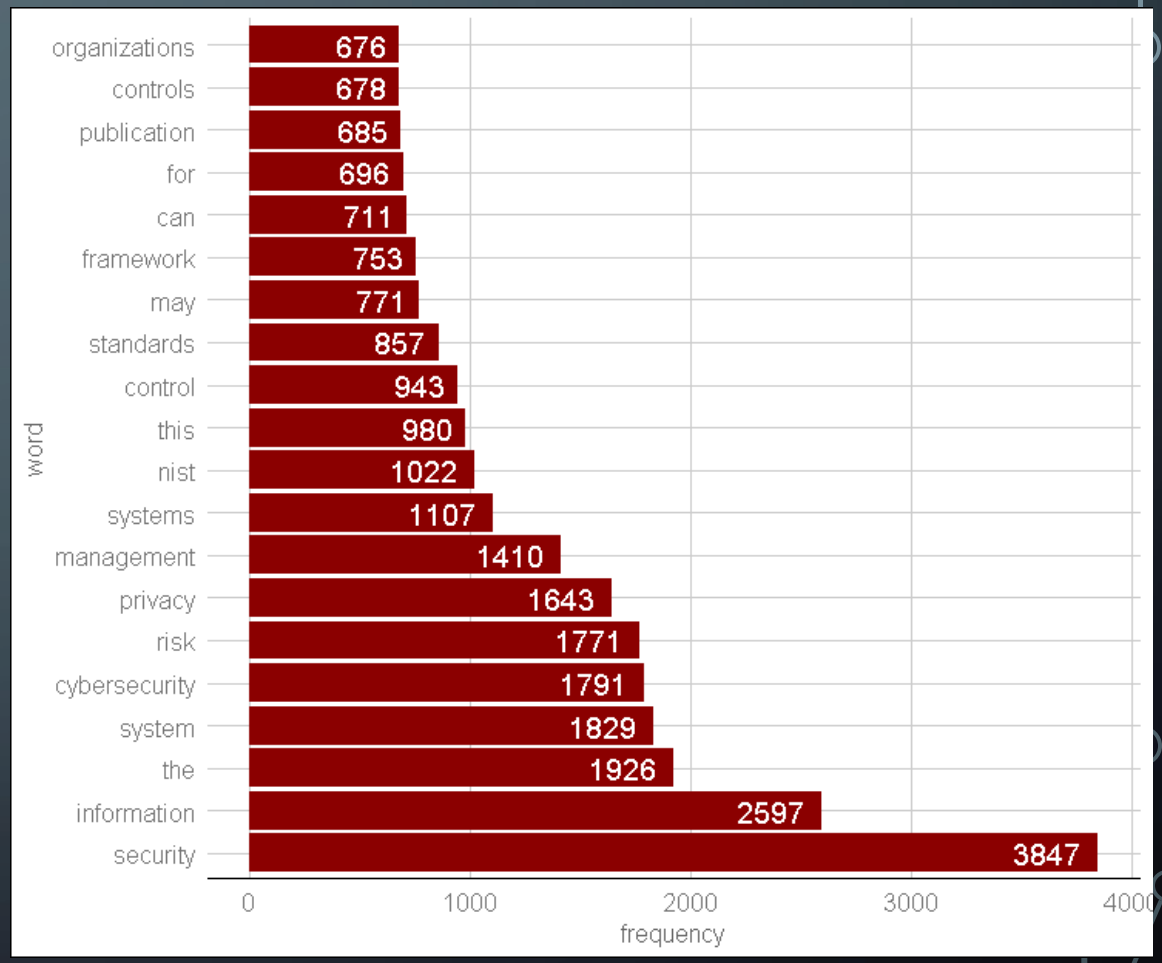
- All data is cleaned by:
  - Setting to lowercase
  - Removing punctuation
  - Removing English stop-words
  - Stemming/truncating words

METHODOLOGY

- Overarching ideas, themes, and policy goals
  - Key Terms
  - Key Phrases
  - Preconstructed dictionary of Cyber Policy Categories
  - Cross Tabulation of Key terms and phrases against dictionary

KEY TERMS





Term frequency utilized TM package, visualization utilized ggplot2

*Multiple attempts to clean Industry corpus of 'stopwords' and 'removewords' still rendered the visualization shown.

KEY PHRASES OF THE DOD CORPUS

	collocation	count
1	dod compon	552
2	communic system	336
3	ENCLOSURE dodi	260
4	chang ENCLOSURE	182
5	depart defens	226
6	accord refer	242
7	secur control	262
8	cloud comput	146
9	defin refer	234
10	joint forc	180

	collocation	count
1	nation secur system	102
2	defens network informat	31
3	operations manag plan	16
4	joint chief staff	113
5	dod informat secur	21
6	accord author dod	10

Quanteda Package Utilized to find common 2 and 3 word phrases

*only 6 3 word collocations met required number of >=10 instances across all documents

*words shortened due to stemming for analysis

KEY PHRASES OF THE INDUSTRY CORPUS

	collocation	count
1	security privacy	942
2	risk management	641
3	this publication	411
4	publication available	373
5	cybersecurity framework	341
6	authorizing official	301
7	senior agency	233
8	NIST SP	253
9	cycle approach	194
10	information security	514

	collocation	count
1	standards provide security	23
2	agency official privacy	115
3	a system life	188
4	security management systems	17
5	cycle approach security	186
6	system privacy officer	63

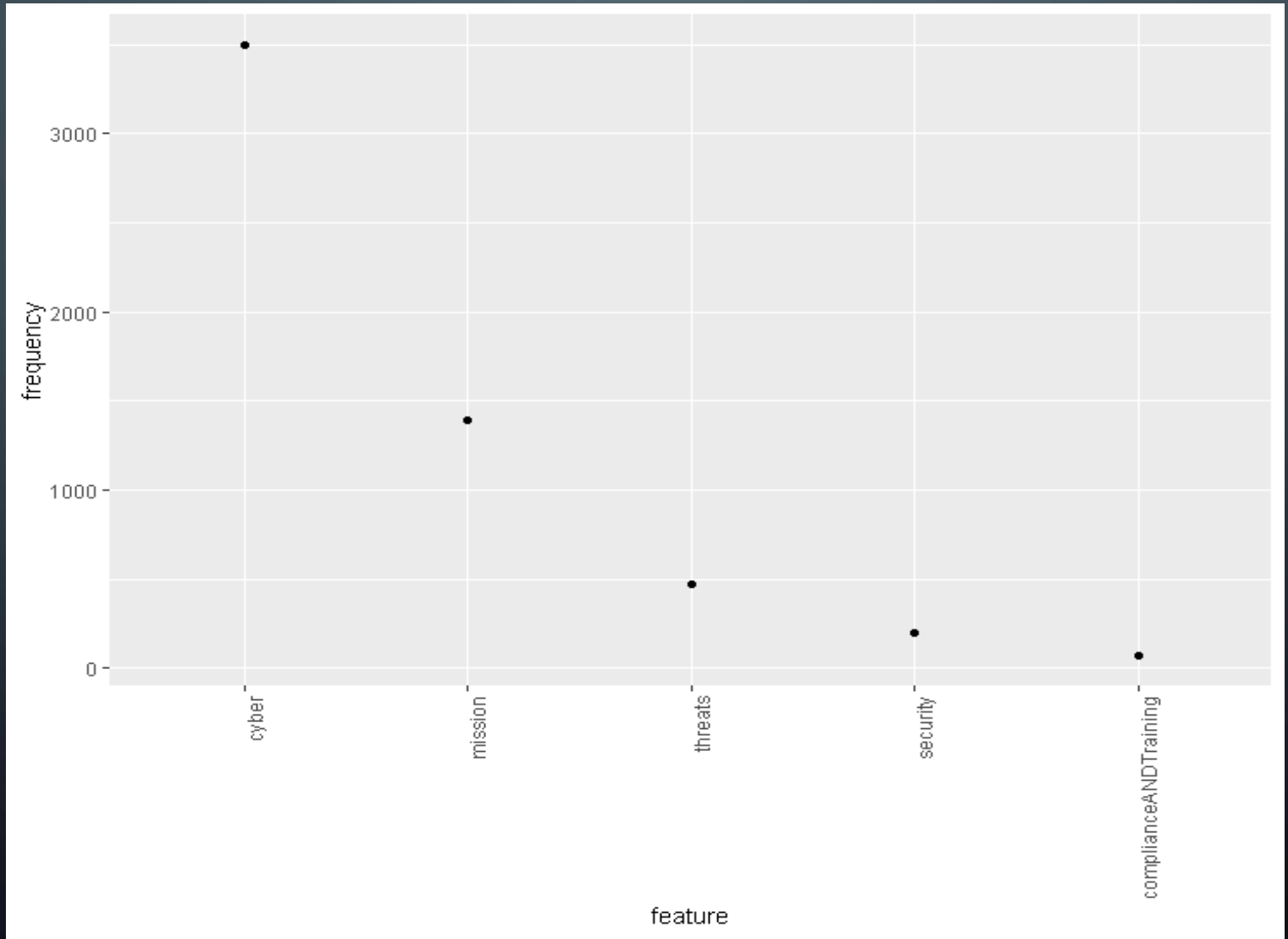
Quanteda Package Utilized to find common 2 and 3 word phrases

*only 6 3 word collocations met required number of >10 instances across all documents

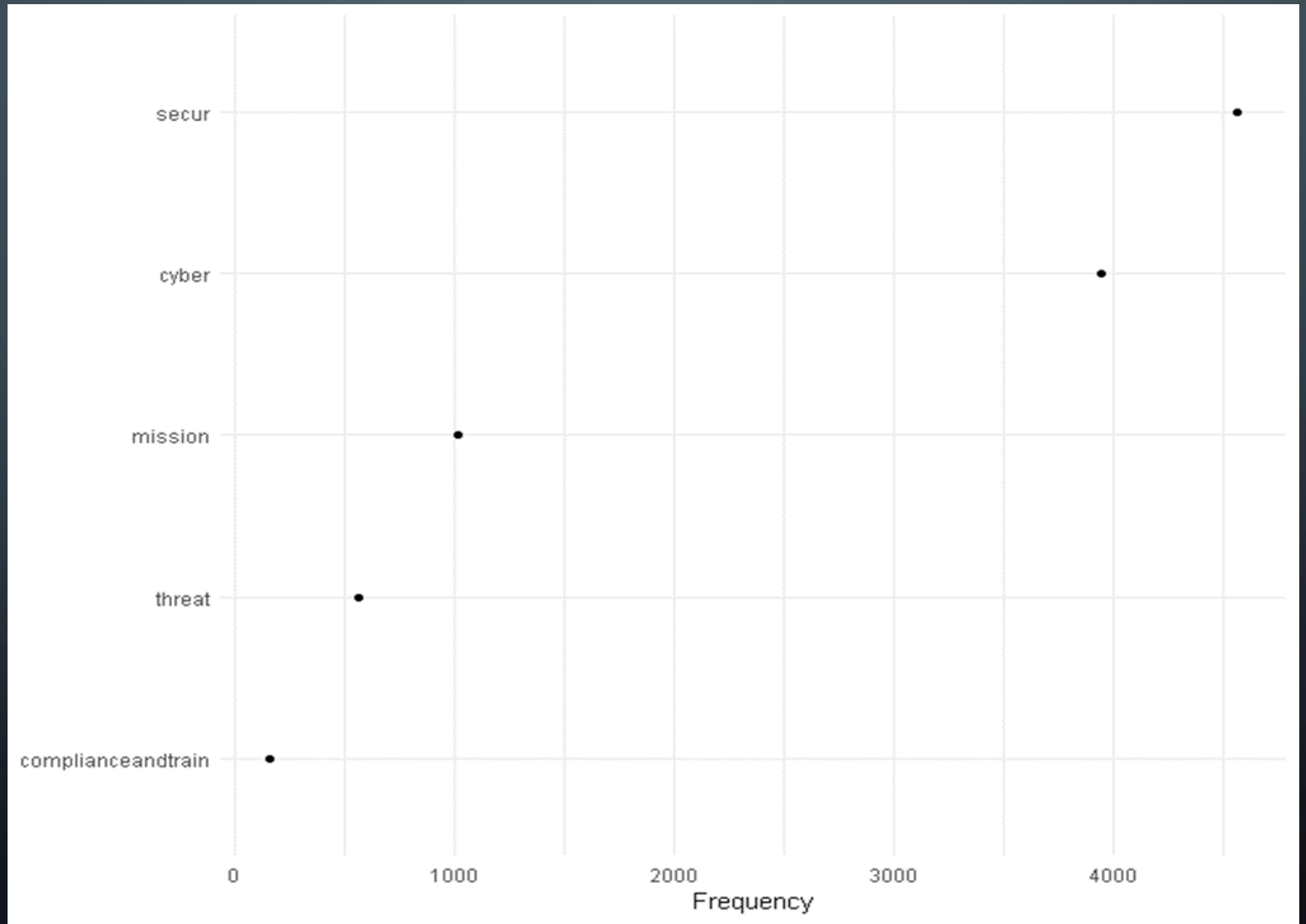
DICTIONARY

1	Cyber	Hardware, software, systems, digital infrastructure, network, computer, server, switch, router
2	Threats	Intrusion, vulnerabilities, weakness, hacker, hacking, botnet, DDoS, malware, spam, phishing, pharming, spillage, leak,
3	Security	Firewall, antivirus, two factor authentication, verification, Host Based Security System (HBSS)
4	Mission	Operation, operational, tactical, strategic, deployed, forward, unit based
5	Compliance & Training	Qualified, certified, credentialed, CCNA, CISSP, NET+, SEC+, security manager, information assurance manager, network administrator

APPLICATION OF THE DICTIONARY TO DOD CORPUS



APPLICATION OF THE DICTIONARY TO INDUSTRY CORPUS



FINDINGS

- Consistencies – Prevailing theme of system security
  - Meets basic logical assumption for cybersecurity policy
    - No real research value added
- Inconsistencies
  - The themes represented through the dictionary application
- The extent to which industry standards are represented by DOD cybersecurity policy
  - indeterminable from the findings.
- Prevailing themes
  - Were determined and applied via the developed dictionary, validating the assumption.

END