CS6000 Journal Assignment 3

Brian D. Wisniewski

September 17, 2019

1 Process Overview

My approach to quickly skimming these articles was derived from a technique I remember from a previous class many years ago. The instructor had termed it "predatory reading" and it consisted of reading the Title, Authors (and author background if available for context) the abstract, introduction, or first paragraph, and then the first sentence and last 2 sentences of each paragraph through the conclusion. Diagrams, drawings, and illustrations should be scanned and any questions noted.

2 Critical / Creative Reads

1. Critical / Creative Reading - The author revisits the concept of the Maginot Line as originally envisioned. Defense is meant to create opportunity for offensive action or in the case of cybersecurity, proactive measures. [1]
2. Critical / Creative Reading - The author outlines the requirements of international law in defining the potential of collateral damage with regards to cyberspace operations. The article points out that many of the concerns around collateral damage are overblown and when compared to conventional secondary and tertiary impacts, may actually hold more options for military leaders to avoid unnecessary casualties. [2]
3. Critical / Creative Reading - Cyber Threat Characterization is important as we consider threat modeling and vulnerability assessment. Numerous frameworks offer a way to assess the cyber threat in a standardized way. The importance of incorporating these approaches into systems development early in the lifecycle is noted.[3]
4. Critical / Creative Reading - The authors describe 3 approaches to leveraging "manueverable applications." Dynamic resource provisioning can utilize an approach similar to that used in academic environments for Hadoop scheduling. The second approach cites Software Defined Networking as a key capability required for application optimization. Finally, creation of a distributed application environment offers the potential of a shifting attack surface.[4]
5. Critical / Creative Reading - The author argues that the traditional checklist

approach must evovle. It requires a more proactive approach where authoritative frameworks are used as the foundation, but organizations must apply unconventional controls on a dynamic basis based upon the evolving threat. [5]

3 References

References

[1] R. Rothrock, "Digital network resilence: Surprising lessons from the maginot line," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title and Author. Author not familiar. Reference of Maginot Line again points to strategic / policy article. Maginot Line = Complacency - crux of the article. Para. 1. 10 - 50 sec. Skimming first and last 2 sentances of each paragraph. Significant historic analysis. Twist in Para. 6. Maginot Line gets a bad rap. 50 - 90 sec. Re-reading Para. 6 fully and continuing through. Cites actual purpose of Maginot Line as to free manpower for more offensive operations elsewhere - analagous to automated SIEM / IPS allowing analysts to focus on more suspect / subtle IOC's, etc. 90 - 120 - Ran out of time - Marked article to read more thoroughly. The focus on resilience is intriguing. Critical / Creative Reading - The author revisits the concept of the Maginot Line as originally envisioned. Defense is meant to create opportunity for offensive action or in the case of cybersecurity, proactive measures.

[2] L. M. G. Bertoli, "Cyberspace operations collateral damage - reality or misconception?," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title and Authors. 10 - 60 - Scenario approach to narrative. Last sentance - first Para. summarizes the Author's thoughts - cyberspace operations collateral damage risk appears overblown and can be addressed in a manner similar to what is applied to the kinetic realm. Narrative / Scenario approach of article causing First line / last 2 lines method not efficient in determining an underlying theme. 60-80 sec. noted that the authors cite doctrine and international law. Strategic focus. 80-100 sec. Several paragraphs addressing risk of 2nd and 3rd order effects. 100-110 sec. - Good diagram on General Collateral Damage Taxonomy. 110 - 120 - ran out of time, but noted the authors propose a formula to help decision makers with weighing the collateral damage risk (CDR). Marked article to read more thoroughly. The importance of legal impact, particularly around cyber-physical systems, is part of my focus. Critical / Creative Reading - The author outlines the requirements of international law in defining the potential of collateral damage with regards to cyberspace operations. The article points out that many of the concerns around collateral damage are overblown and when compared to conventional secondary and tertiary impacts, may actually hold more options for military leaders to avoid unnecessary casualties.

[3] E. D. K. Jabbour, "Cyber threat characterization," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title, authors, and first paragraph. 10-25 sec. mention of cyber threat models and the Cyber Red Books. 25-50 first sentance, last 2 of each paragraph. NIST, capability, access, intent. 50 - 70 sec. Mention of trends, 2005 GAO threat table, 70 - 100 sec. focus on 10 dimensions of the cyber threat, noted mention of the Byzantine Generals Program for failure analysis, threat actors embedded within the supply chain - a key driver for my own recent experience. 100 - 120 - ran out of time - Marked article to read more thoroughly. The authors did a good job of outlining supply chain risks. Critical / Creative Reading - Cyber Threat Characterization is important as we consider threat modeling and vulnerability assessment. Numerous frameworks offer a way to assess the cyber threat in a standardized way. The importance of incorporating these approaches into systems development early in the lifecycle is noted.

[4] A. A. W. Moody, "Manueverable applications: Advancing distributed computing," *Cyber Defense Review*, vol. 2, no. 3, 2017. 15 sec. Title, Authors, Abstract. 15 - 30 sec. Discussion of manuevrable applications. distributed / parrallel systems. 30 - 90 sec. focus on resource provisioning, application optimization, and cybersecurity enhancement. Mirrors similar work we are doing on the civilian side with PLC's. 90 - 120 sec. Marked for additional review. The concepts around Hadoop optimization have potential applicability. Critical / Creative Reading - The authors describe 3 approaches to leveraging "manueverable applications." Dynamic resource provisioning can utilize an approach similar to that used in academic environments for Hadoop scheduling. The second approach cites Software Defined Networking as a key capability required for application optimization. Finally, creation of a distributed application environment offers the potential of a shifting attack surface.

[5] J. Routh, "The emergence and implications of unconventional security controls," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, author, and intro. Recognize the author from a previous conference. 10 - 50 sec. Skimmed first sentance and last 2 of ea. paragraph. Discusses Uncovnentional Controls. Didn't immediately understand. 50-70 sec. went back and re-read the inital definition offered and subsequent paragraphs. 70 - 120 - began reading at length and ran out of time. Marked article to read more thoroughly. As a former delegated Authorizing Official, I am particulalry interested in this area. Critical / Creative Reading - The author argues that the traditional checklist approach must evovle. It requires a more proactive approach where authoritative frameworks are used as the foundation, but organizations must apply unconventional controls on a dynamic basis based upon the evolving threat.

[6] D. Barrett, "Cybersecurity: Focusing on readiness and resiliency for mission assurance," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Read Author and Title and first line. 1-star Navy Admiral - likely not techni-

cal. 10-50 sec. scanning first paragraph, second paragraph - last line, 2nd paragraph likely summarizing the article. 50 - 100 sec. Skim first and last sentances of each paragraph. Noted mentioned of "cyber key terrain" in para. 4. Noted organizational structure of Cyber Protection Teams cited in Para. 10. 100-120 sec. Last 2 sentances summarizes the article well. Technique and Policy focused overall. Discard. The article is interesting but not applicable to my current focus.

[7] A. C. T.Casey Fleming, E. Qualkenbush, "The secret war against the united states," *Cyber Defense Review*, vol. 2, no. 3, 2017. 15 sec. Multi layered title. 3 authors. Recognize 1 from previous projects. 15-60 sec. Pearl Harbor analogy. Last sentances, paragraph 2 likely outlines overall article. Assymetric Hybrid Warfare cited. Para. 5 cites Sun Tzu - clearly a strategic / policy article. 60 - 120 sec. Noted the authors Call to Action. Discard. The article is interesting but not applicable to my current focus.

[8] O. Sultan, "Combatting the rise of isis 2.0 and terrorism 3.0," *Cyber Defense Review*, vol. 2, no. 3, 2017. 15 sec. Title and Author. Author not familiar. Subject matter is over several tours in Middle East. 15 - 60 seconds. Skimming first sentance and last 2 of each paragraph. Appears philisophical. 60 - 100 seconds - Mention of Al-Queada Inspire magazine derails my skimming, but overall the focus of the article seems to be the threat of Cyber Terrorism and the use of what the military terms Information Operations through Social Media, etc. 100 - 120 Noted study conducted by Author on radicalization and social media. Author calls for more strident steps to tackle the growing ISIS threat online now. Last para., last line. Discard. The article is interesting but not applicable to my current focus.

[9] G. A. Crowther, "The cyber domain," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10. Title and Author. 10-15 sec. first few sentances. Focus on cyber as domain. strategic article. Last 2 sentances of first Para. provide a succinct summary of article and the author's main points. 15-60 first sentance and last 2 of each paragraph. Traditional point and arguments to support that point (or disprove a negative point). 60-80 sec. review diagrams. fairly straightforward. 80 - 100 mention of cyber crime in the context of its impact on broader strategic military operations catches my attention. 100 - 120 Skimmed through last several paragraphs noting references to recent Chinese information warfare efforts and Russian interference. Discard. The article is interesting but not applicable to my current focus.

[10] R. Martins, "Anonymous' cyberwar against isis and the asymmetrical nature of cyber conflict," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title, Author, and Abstract. Last sentance of abstract likely summarizes article. 15 sec 5 asymetrical characteristics. 15 - 60 skimming paragraphs on background of Anonymous, ISIS, and asymetric warfare. Note the phrase "cyberspace can be a great equalizer". Summary of various efforts by Anonymous against ISIS at its height. Mention of Billy Mitchell

and analogy for cyber. 60 - 90 - summary of specific targeting of ISIS by Anonymous with total numbers of disrupted accounts, etc. 90 - 120 Conclusion notes conflicts in cyberspace will require a "protracted, persistent, and committed effort." Discard. The article is interesting but not applicable to my current focus.

[11] M. M. R. B. J. Kallberg, W. Blake Rhoades, "Defending the democractic open society in the cyber age - open data as democratic enabler and attack vector," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title, Authors, and first 2 para. Recognize Kallberg. 15 sec. - last sentance para. 2 - focus of article. 15 - 60 reading first sentance, last 2 of each paragraph. 60 - 90 revisting Para. 4 - quote from Abraham Lincoln caught my eye. Article offers that in order to defend democracy, we need to be more open and provide for an informed electorate. 90 - 110 - Impact of internationalization and globalization. Multiple data sources provided by the USG. 110 - 120 conclusion. Very much a policy article. Discard. The article is interesting but not applicable to my current focus.

[12] T. Waters, "Multifactor authentication - a new chain of custody option for military logistics," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title, author, and first 3 paragraphs. Offers additional options for MFA beyond traditional use cases. 10-60 seconds - very easy article to skim. Essentially an argument to apply MFA to military logistics to reduce tampering, sabotage, etc. 60 - 120 seconds. Finished entire article and revisited his "Supply Chain of Custody" points. Good article. Discard. The article is interesting but not applicable to my current focus.

[13] R. Schrier, "Demonstrating value and use of language - normalizing cyber as a warfighting domain," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, author, and first several sentances of Abstract. Last sentance, first Para. likely provides overview of article. 10 - 70 sec. First sentance, last 2 of each para. method. Noted the importance of language and interpersonal communications (particularly with industry-specific terms) as a factor in understanding cyber's impact. 70 - 90 sec. reviewed the description of the change from Communications Task Orders to a traditional format - something I recall being involved with. 90 - 120 sec. Overall article seems to explain the early days of USCYBERCOM and some of the reasons it took the approach it did. Discard. The article is interesting but not applicable to my current focus.

[14] N. Blacker, "Winning the cyberspace long game - applying collaboration and education to deepen the u.s. bench," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, author (NDU Faculty member), and initial summary para. Focus on collaboration challenges. 10 - 50 sec. Para. 3, last sentance reveals underlying reason for the article - request that National Defense University College of Information and Cyberspace be designated as the primary institution to educate collaborative teams, etc. 50 - 90 sec.

honestly began to skim faster - clearly a self serving position paper. 90 - 120 - agree with need for collaboration, but not with the arguments presented for NDU to be the clearinghouse for such efforts. Discard. The article reads like a grant or funding proposal.

[15] S. H. J. Baker, "The cyber data science process," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, authors, and intro. Served under MG Baker previously. Acerbic but intelligent individual. 10 - 70 sec. skimming over. Focus will be on "How" of cyber data science within the Army. Need to collect and understand the data avaialble, but the scale of the Army networks is vast. Industry best practices. intelligence collection and targeting. 2 analogs. Several diagrams. 70 - 100 revisit diagrams. Most are familiar. Proposes Data Science Workflow for the Army. 100 - 120 - Ran out of time. Marked article to read more thoroughly. The discussion around the need for data science within our formations is something I do agree with.

[16] B. Bialy, "Social media - from social exchange to battlefield," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, author, Introduction. 10 - 50 - social media and its impact on strategic communications. Early examples BBS, friendster, social media mining - Facebook scandal. Privacy issues. Marketing. Noted in Para. 15 - how many folks use social media for news. 50 - 90 - Review of Para 15 and on - citing the emergence of social media as a challenge to mainstream media. Grassroots journalists. "anything can become news". Social cyberattacks. Weaponization of social media. Cited hacked AP Twitter account and false report of explosion at White House. 90 - 120. Offers 5 recommendations. Discard. The article would be better oriented toward a strategic journal from one of the War Colleges.

[17] D. D. Goss, "Operationalizing cybersecurity - framing efforts to secure u.s. information systems," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, author, Abstract paragraph. 10 - 50 - Skimming intro. Information definition. Information sys. security. CIA but including authenticity and non-repudiation. Noted mention of "quantifying the value of the cybersecurity program". 50 -60 - Risk management. Multiple risk analysis methodologies mentioned. 60-90 Economics of cybersecurity. Where, how to demonstrate value? Human factor within cybersecurity. 90 - 120 - Conclusion - Cybersecurity needs holistic approach. Discard. The article is interesting but not applicable to my current focus.

[18] B. S. A. Hall, "Direct commission for cyberspace specialities," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, authors, Abstract. Know authors. 10 - 50 sec. first sentance / last 2 method. Direct commission solves short term manpower shortage. Pros - quick, easy. Cons - Likely creating longer term headaches with inexperienced, improperly vetted leaders. 50 - 90 - compare with Medical Corps however no central civilian licensure/board process for cyber. Cites Defense Digital Service as a positive example. Pilot program overview. Article is simply a supporting proposal.

90 - 120. Revisit diagrams. Discard. The article is interesting but not applicable to my current focus.

[19] K. S. P. Hayden, D. Woolrich, "Providing cyber situational awareness on defense platform networks," *Cyber Defense Review*, vol. 2, no. 2, 2017. 10 sec. Title, authors, abstract. Last 4 sentances summarizes article. 10 - 60 Threat overview, how to categorize, Jeep example, 1553 Bus mentioned, 60 - 90 defense platforms heterogenous nature provides vast attack surface, 90 - 120 BAE systems authors, offers pitch for 1553 Bus interoperability, but refreshingly, no direct BAE pitch. Discard. The article is interesting but not applicable to my current focus.

[20] N. Sambaluk, "Making the point - west point's defenses and digital age implications, 1778-1781," *Cyber Defense Review*, vol. 2, no. 3, 2017. 10 sec. Title, author, Abstract - 10 - 50 sec. interesting analogy of British unable to "brute" defensive works. Used insider threat - Benedict Arnold. 50 - 120 - got caught enjoying the history and ran out of time. Violated my first sentance / 2 last sentance method. Discard. The article is interesting but not applicable to my current focus.

[21] C. W. P. Frost, C. McClung, "Tactical considerations for a commander to fight and win in the electromagnetic spectrum," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Authors and Editor, Abstract. US too focused on CI over past 18 years, adversaries have leap-frogged EW capabilities. 10 - 70 sec. Loss of radio discipline over past 2 decades. Overmatch by US in Iraq/Afghanistan taken for granted. Paper offers critical questions on moving into the near-peer environment. 10 questions. 70 - 90 Re-read the last 3 questions with a focus on spectrum management. 90 - 120 - Conclusion - We need to be prepared to operate in an electronically degraded environment. Discard. The article provides no new information beyond current guidance within the DoD.

[22] J. Pfeifer, "Preparing for cyber incidents with physical effects," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Author, Abstract - Value of TTX's for major cyber/physical incidents. 10 - 50 sec. TTX's between West Point and NYPD/NYFD, etc. Situational awareness key. National Cyber Incident Response Plan - Presidential Preparedness Directive 41, ISAC's, DHS, and Fusion Centers. Incidnet Management. 50 - 90 sec. Summarized incident management. NIMS. Communications is key. Nothing new here. 90 - 120 Conclusion - quote from McChrystal - robustness vs. resilience. Discard. The article is interesting but not applicable to my current focus.

[23] B. Bort, "There is no cyber defense," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Author - Abstract - somewhat cynical. 10 - 80 sec. Overall author touts detection and response. Cites multiple failures in current technologies. Unclear what his final point is. 80 - 120 - re-skimmed the article (not long) trying to figure out if he's pitching a product / service?

Discard. The article is not interesting and not applicable to my current focus.

[24] A. B. S. Henry, "Countering the cyber threat," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Author, Abstract. Focus on information sharing, public / private. One author is crowdstrike President. 10 - 70 sec. Complexity of problem. Need more sharing. Public and PRivate problem. Number of connected devices. Recognition of the problem. Rapidly declassified and anonymized threat indicators, people to act on them. Team sport. 70 - 120 - Revisited final points and conclusion. Essentially uses 9/11 as an analogy for how a coordinated response to cyber must be undertaken.

[25] E. A. E. Yoran, "The role of commercial end-to-end secure mobile voice in cyberspace," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, authors, Abstract. - 10 - 50 - Initial skimming. DHS offering on mobile security framework? Securing voice and data using mobile devices. Global interception of mobile comms not just nation-state issue anymore. 50 - 70 Note on NIST study. Mobile voice threats specifically. DHS report and LTE example. 70 - 90 - diagram review on DHS Mobile Ecosystem Model and IMSI Catcher Concept. SS7 vs. Diameter and vulnerabilities. 90 - 120 Ran out of time. Marked article to read more thoroughly. Aligned with interest in hardware / firmware security.

[26] B. H. H. Arata III, "Smart bases, smart decisions," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Authors, Abstract - Ubiquitous connnectivity. 10 - 40 sec. skimming. IoT discussion. Commercial (not industrial) self-healing networks. 40 - 70 push "data crunching and analytics" closer to the edge. data tranformation curve. IoT and impact on cities, communities. 70 - 90 - review diagrams. 90 - 120 - Overall, better for public safety, infrastructure monitoring, multi-network solutions, Logistics management, waste management, etc. - Ran out of time. Marked article to read more thoroughly. Aligns with interest in industrial automation.

[27] C. Downes, "Strategic blind-spots on cyber threats, vectors, and campaigns," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Author, Abstract - 2016 election. Author is NDU professor. International Relations focus. 10 - 70 - Russian election interference. Active Measures. US had "strategic blind spots" and did not consider threat. Elections are a critical target. IPv6 expansion of target surface area? "first to market" pressures drove down security considerations. PPD 21 left out elections as a CI. 70 - 90 - focused on "Strategy and Strategic Thinking Required as Much as Military Doctrine" section. West's concept of war remains Napoleanic (industrial IMHO). Points to U.S Army infatuation with Operational Art as giving short attention to Strategy. I agree. 90 - 120 - tried to race through the rest but ran out of time. Marked article to read more thoroughly. Aligns with focus on broadly integrating Strategy with our current TTP's.

[28] J. C. E. Kania, "The strategic support force and the future of chinese information operations," *Cyber Defense Review*, vol. 3, no. 1, 2018. 20 sec. Title, Authors, and first paragraph. 20 - 70 Overview of Chinese 2015 Strategic Support Force for information warfare. Shift in Chinese approach. Attempt to adapt against an militarily stronger adversary. Mention of Mandaint APT1 Report. Obama 2015 agreement. removal of peacetime / wartime distinction. 70 - 90 - SSF Leadership structure, similar to STRATCOM minus nukes. Diagrams. 90 - 120 Complex org. structure, but may provide much greater coordination. Discard. The article is interesting but not applicable to my current focus.

[29] M. S. N. Kostyuk, S. Powell, "Determinants of the cyber escalation ladder," *Cyber Defense Review*, vol. 3, no. 1, 2018. 10 sec. Title, Authors, Introduction. Author is from Belfor Center (think tank). Policy focused article. 10 - 50 Ukraine example. Need to communicate escalation ladders and account for differences in culture. 50 - 90 - Ladder similar to during Cold War. 2016 Election discussed. Where does that fit onto the ladder? 90 - 120 sec. Diagram of an example ladder. Discard. The article is interesting but not applicable to my current focus.

[30] J. N. K. Hubbard, "Financial stewardship in the land of "1's and 0's"," *Cyber Defense Review*, vol. 3, no. 2, 2018. 10 sec. Title, Authors, Introduction. 10 - 30 Need to create centralized Major Force Program (MFP) to track and report on investments by DoD cyberspace operations. 30 - 90 - Overview of budget process. Interesting but not currently applicable. Without centralized reporting, funding for cyber remains contentious. Requires greater oversight. SOF cited as a reasonable model. 90 - 120 sec. 3 major recommendations. Discard. The article is interesting but not applicable to my current focus.

[31] D. D. G. L. Wyche, "Attacking cyber: Increasing resilience and protecting mission essential capabilities in cyberspace," *Cyber Defense Review*, vol. 1, no. 2, 2016. 10 sec. Title, Authors, Introduction. 10 - 30 Focus is on Supply Chain Security. Policy focused article. Army Material Command (AMC) 30 - 70 Skimming through. Defense Industrial Base. Test - Assess - Revise. 70 - 100 Cultural changes required. 100-120 Somewhat light on details. Reads like a speech. Discard. The article is interesting but not applicable to my current focus.

[32] M. V. D. Wallace, "The use of weaponized "honeypots" under the customary international law of state responsibility," *Cyber Defense Review*, vol. 3, no. 2, 2019. 15 sec. Title, Authors, and Abstract. Overarching theme - is placing malware in Honeypots and allowing an adversary to exfiltrate them against international law. 15 - 50 sec. define honeypot. Appears original audience was non-technical. Cite the Tallinn Manual 2.0. and NATO CCDCOE. Article distinguishes comments as "law as it exists" vs. "law as it should be". 50 - 80 sec. Legal defenses for perpetrators of Weaponized

Honeypot. International law is meant to govern STate to STate not non-state actors. Doctrine of countermeasures vs. Doctrine of Necessity. Self Defense. 80 - 120 - Overall, it depends. Discard. The article is interesting but not applicable to my current focus.

[33] A. Cohen, "Effective cyber leadership: Avoiding the tuna fish effect and other dangerous assumptions," *Cyber Defense Review*, vol. 3, no. 2, 2018. 10 sec. Title, Author, opening joke? 10 - 30 focus on leadership and motiviation. Directing people. 30 - 50 Use of the Anthrax attacks as a case study scenario. 50 - 100 tuna can sitting on a keyboard. unrealistic demand. lack of clarification. 100 - 120 - concludes with some quippy statements. Discard. The article is interesting but not applicable to my current focus.

[34] K. Dill, "Cybersecurity for the nation: Workforce development," *Cyber Defense Review*, vol. 3, no. 2, 2018. 15 sec. Title, Author, and Abstract. 15 - 30 Problem statement and historic examples. CBRN response example. 30 - 90 Skimming first sentance/last 2. Civil Air Patrol? Kids programs. Hak4Kidz. JROTC tie in. 90 - 120 - Conclusion to create a Civil Cyber Force modeled after Civil Air Patrol. Discard. The article is interesting but not applicable to my current focus.

[35] M. K. K. Tresh, "Toward automated information sharing california," *Cyber Defense Review*, vol. 3, no. 2, 2018. 15 sec. Title, Authors, Introduction. Cal-CSIC State organization. 15 - 50 - Skimming. State Gov. Exec. Order. Distributed structure. Outputs must be actionable. Key challenges. 50 - 90 - solution proposed. avoiding email fatigue. SEIM. Threat list integration. Automation key. 90 - 120 - Pilot effort. Primary and alternate model for large and small agencies needed. Discard. The article offers an information sharing model, but not applicable to my current focus.

[36] F. Katz, "Breadth vs. depth: Best practices teaching cybersecurity in a small public," *Cyber Defense Review*, vol. 3, no. 2, 2018. 10 sec. Title, Author, Abstract. Breaches overview. NSA accredited program created, courses, and pedagogical methods. 10 - 50 Creation of a small IT program. alignment with NSA curriculum. Stackable curriculum. Market demands - nearby military bases. Postsecondary certificates and credentials. 50 - 90 close mapping of all courses to NSA-CAE Knowledge Units (KU's). 90 - 120 balance of depth and breadth. consolidation with another university will likely drive further enrollment. Discard. The article is interesting but not applicable to my current focus.

[37] C. Lotrionte, "Reconsidering the consequences for state-sponsored hostile cyber operations under international law," *Cyber Defense Review*, vol. 3, no. 2, 2018. 10 sec. Title, Author, and Introduction. cyber acts that fall below level of war vs. those above. 10 - 60 - ambiguous nature of law related to cyber. definitions. pace of tech changes. gray zone area of conflict. 60 - 90 - further definitions of war and short of war. spirit of existing law as guidance. Cite Tallinn Manual 2.0 again. Non-binding. UN Charter. 90-120

- ran out of time. Article is extremely detailed. Marked article to read more thoroughly. The article is well written and very detailed.

[38] M. G. M. Span III, L. Mailloux, "Cybersecurity architectural analysis for complex cyber-physical systems," *Cyber Defense Review*, vol. 3, no. 2, 2018. 20 sec. Title, Authors, and Abstract. 4 overall goals of article. 20 - 90 sec. Survey of architecture models, both open and private. UAF? Also RMF and legacy systems assessments. Boundary analysis. FMEA and Attack Path Analysis. 90 - 120 Assessment discussion. Ran out of time. Marked article to read more thoroughly. The article matches up well with my focus on industrial automation security.

[39] C. L. P. Nakasone, "Cyberspace in multi-domain battle," *Cyber Defense Review*, vol. 2, no. 1, 2017. 10 sec. Title, Authors, and Introduction. 10 - 50 WWII analogy with Britain. Nothing in the concept is new. 50 - 90 discussion of way of thinking. Focus on ensuring an offset with adversaries. defense of networks, data, weapons systems. deliver cyber effects. Integrate the full capabilities. 90 - 120 Conclusion, analogy from Intro. continues. Discard. The article actually outlines emerging doctrine, but is not applicable to my current focus.

[40] J. B. K. Alexander, J. Jaffer, "Clear thinking about protecting the nation in the cyber domain," *Cyber Defense Review*, vol. 2, no. 1, 2017. 15 sec. Title, Authors, and Intro. digital battleground. proactive approach needed. US not addressing the situation seriously enough. 15 - 50 Accelerated growth of technology. Cyber crime, espionage, theft of intellectual property. 50 - 90 Acts of war in cyber? How to respond. gray area conflict. sharing and collaboration will be key. 90 - 120 Critical that key decisions are made. Stay ahead of the problem. Discard. The article is a bit too much on need for collaboration.

[41] A. Brantly, "The violence of hacking: State violence and cyberspace," *Cyber Defense Review*, vol. 2, no. 1, 2017. 15 sec. Title, Author, and Introduction. 15 - 30 sec. Cyber violence? Definitions. Threatened and applied. "More akin to subversion and manipulation". 30 - 60. International relations focus. Article appears oriented at policy. 60 - 90. William Gibson quote. Using non-kinetic means to achieve forcibly taking something? Blockade - physical or virtual? Clausewitz. 90 - 120 sec. violence in the shared information space. Discard. The article is interesting but not applicable to my current focus.

[42] G. A. C. Bronk, "Encounter battle: Engaging isil in cyberspace," *Cyber Defense Review*, vol. 2, no. 1, 2017. 15 sec. Title, Authors, and Introduction. ISIL (ISIS) in cyber. Similar to previous article. 15 - 70 sec. Skimming on coaltion challenges. Kurdish issue. Unique force mix. Potential spill over. Social media as primary channel in Para. 11. 70 - 100 sec. ISIL narrative and equipment (e.g., GoPro cameras, etc.) Twitter, Instagram. Radicalization via cyber. "Contemporary and future conflict will be dominated by drones,

special operations forces (SOF), and cyber." Online recruiters. 100 - 120 sec. Historic analogies. Doxing concerns. Policy options. Discard. The article is interesting but not applicable to my current focus.

[43] C. W. J. Healy, L. Mcinnes, "Bridging the cyber-analysis gap: the democratization of data science," *Cyber Defense Review*, vol. 2, no. 1, 2017. 10 sec. Title, Authors, Intro. Crowd-source data science? 10 - 60 sec. growth of data. "wisdom of the crowd"? shared collaborative workspace. Leverage machine learning universally? 60 - 100 sec. Model T analogy. Machine learning - potential maintenance nightmare - Google paper 2014. Python and Jupyter. 100 - 120 sec. approach could help overwhelmed cyber analysts. Discard. The article is a bit too technical for my current focus.

[44] M. Kolton, "Interpreting china's pursuit of cyber sovreignty and its views on cyber deterrence," *Cyber Defense Review*, vol. 2, no. 1, 2017. 15 sec. Title, Author, and Introduction. Very similar to previous article. Author is U.S. Army (vs. researcher). 15 - 60 sec. 3 goals of article. China objective in cyberspace. China cyber strategy. Cyber detterance efficacy against China. Creation of SSF. 60 - 90 sec. Shift of Internet governance. China is focused on control. Cites CSIS studies on China. Advanced military as key goal. 90 - 120 sec. Strategic / Policy article. Ends Ways Means. Discard. The article is interesting but not applicable to my current focus.

[45] N. Sambaluk, "The challenge of security: West point's defenses and digital age implications, 1775-1777," *Cyber Defense Review*, vol. 2, no. 1, 2017. 15 sec. Title, Author, and Introduction. Serves as initial article found in later volume focussed on 1778-1781. 15 - 60 Historic analogy as it relates to cyberdefense. Layered defense similar to "defense in depth". Revolutionary War planners recognized military principle of defenses buy time. 60 - 90 - Review Map. Analysis of the defense. 90 - 120 Coordinated action was key. No defense is perfect. Construction of defense is a deliberate activity. Discard. The article is interesting but not applicable to my current focus.