AY 2018-2019 USCYBERCOM Research Topics

26 July 2018

The overall classification of this briefing is: UNCLASSIFIED

Introduction

- US Cyber Command hosted its inaugural Cyberspace Strategy Symposium at National Defense University on February 15, 2018.
- As an output of this symposium, **a list of 52 questions** for scholars, students, and members of DOD to inform research at civilian and military institutions of higher education, think tanks, and other research bodies. US CYBERCOM welcomes any products that respond to these topics. (2018 Cyberspace Strategy Symposium Proceedings)
- The list of topics is maintained by the USCYBERCOM J5 Plans, and Policy Directorate and provided to the Joint Staff J7 on an annual basis to facilitate the widest dissemination within DOD Professional Military Education Channels

Topic Categorization

2018 Symposium Panel Categories

- Cyber and the Information Environment
- Speed and Agility for Defense and Offense
- Cyber Persistence
- Integrating Cyberspace Operations into the Joint Force
- Defend the Nation

2018 DOD Cyber Strategy Lines of Effort (LOEs):

1. Empower timely integrated cyber operations
2. Support DoD and Partners with tailored intelligence
3. Transform Network and system architecture
4. Develop next generation capabilities
5. Protect and advance DoD competitive advantage through private sector partnerships
6. Integrate joint information effects
7. Sustain a ready cyber workforce
8. Deter adversaries and and assure critical missions

Broad Questions for Study and Analysis

1. What can we learn from our allies to inform our strategy, operations, organization, and processes?

2. How can we measure success and performance on the cyber battlefield?

3. What is the value of cyberspace operations?

4. What is (and should be) the role of DOD in defending our nation from cyberspace threats?

Cyber and the Information Environment

5. What is the current relationship between information operations (IO) and cyberspace operations?

6. What are the legal and policy changes needed to integrate information operations with cyberspace operations?

7. What are the resources, capabilities, authorities, and partnerships needed to conduct cyberspace operations outside areas of hostility?

8. How can USCYBERCOM augment the nation's ability to conduct strategic influence operations?

9. The intelligence requirements for successful information operations are not accounted for in the kinetic targeting model. How can we increase intelligence support for IO targeting and do it at scale? What structural issues (databases, training, etc.) exist that prevent this ramp up in intelligence support?

10. How can we predict adversary behavior in cyberspace? What trends and insights can we leverage to form such predictions? Can we use that information to destabilize or grapple with the adversary?

Cyber and the Information Environment

- 11. What does a whole-of-society defense in cyberspace look like?
- 12. Can Joint Task Force-Ares, stood up to support C-ISIS operations, serve as a model for scaling support for operations? If so how?
- 13. How would seeing information as basis for power diplomatically, military, and economically change the way we approach the application and assessment of national power?
- 14. What actions in cyberspace fall under traditional military activity? Can DOD use this to legitimize its cyber activities?
- 15. How do our adversaries think about IO and cyber information operations? How is it similar or different from U.S. views? What are the implications for relative advantage?
- 16. How can we organize our forces so that the military can target and execute information operations through cyberspace outside the area of conflict?
- 17. What methods exist to depict the scale of activities by cyberspace adversaries for intelligence professionals?
- 18. From an IO perspective, how much of a departure from traditional IO is what we are now seeing discussed in the news daily?

Speed and Agility for Defense and Offense

19. How can we manage our data to ensure rapid and timely support to commanders' decision making?

20. How does continuous engagement with adversaries change if DOD shifts from a war-focused mindset to a competition-focused mindset?

21. How can we incorporate support elements at every echelon to enhance cyberspace operations? Current model integrates different aspects of support at different echelons (strategic, operational, and tactical).

22. How do we more effectively leverage intelligence and information to pursue our adversaries?

23. Is attribution at a tactical level irrelevant to defensive cyberspace operations? What are the benefits and costs to pursuing and tracking attribution?

- 24. How do you articulate the risks for commanders at echelon to make better decisions?
- 25. How should we modify or adapt plans, policies, and processes to achieve speed and agility?

Cyber Persistence

26. What dynamics from information technology have led to this new, distinguishable domain of cyberspace? Why do previous constructs fail to fit to the realities of cyberspace?

27. What is the role of non-security seeking, security-relevant actors in securing the nation? What do they contribute to national security?

28. What has fundamentally changed in cyberspace since the time USCYBERCOM stood up? How do those changes create challenges for policy, strategy, and competition with adversaries?

29. Where do cybersecurity and cyberspace operations fit into US grand strategy? Into the

strategies of our adversaries?

30. How do we enable cyber forces, in peacetime, to conduct cyberspace operations as traditional military activities?

31. What is the role of the private sector in seizing and maintaining the cyber initiative?

Integrating Cyberspace Operations into the Joint Force

32. Can, and should, the U.S. military implement the Australian military's model for cyberspace?

33. How can changes in the intelligence apparatus improve the support for foundational system analysis and targeting to more effectively employ high demand/low density teams?

34. Is it extremely difficult to perform adversarial threat modeling, especially in cyberspace? How can USCYBERCOM bridge that gap and provide a more accurate threat picture to the USG?

35. How did the transition to a "calls for fires mission" change USCYBERCOM support to CCMDs?

- 36. How does the application of IGL, without reference to OGL, effect cyberspace operations and national objectives?
- 37. How can the services coordinate the use of cyberspace capabilities, the IGL/OGL, and exposed Tactics, Techniques, and Procedures?
- 38. How can and should the military calculate and communicate collateral damage assessments for cyberspace operations?
- 39. With each service developing cyber capabilities, how do we minimize or eliminate redundancies, overlap, and waste?

Defend the Nation

40. How can society be encouraged and incentivized to protect cyberspace?

41. What is DOD’s history with the defense of the nation mission? Why is it not in our “DNA”?

42. Can and should DOD defend the civilian critical infrastructure upon which it relies to execute its missions?

43. Is the war on drugs an appropriate analogy to cyberspace as an example of the “home game” needing the “away game” to defeat external threats to a permeable society?

44. Is DOD letting down its industry partners and/or companies outside the Defense Industrial Base (DIB)? How can we remedy this?

45. If USCYBERCOM had the authority, in the time of an emergency, to support Critical Infrastructure and Key Resources (CIKR) companies, what type of units would be supporting? How would they integrate into steady-state operations?

46. How do government advisories and guidance raise the bar in security for critical infrastructure? How can the government more effectively shape security rather than merely react to events?

Defend the Nation

47. How can the private sector leverage the operational capacity resident in the CNMF? What methods can help evaluate approaches to integrate the CNMF in the defense of critical infrastructure?

48. What are the implications of a standing DSCA request for support to CIKR from USCYBERCOM?

49. How do you define an act of significant consequence in cyberspace? What is the role for USCYBERCOM in preventing these acts?

50. Emergency response begins at the local level and escalates to the state and federal levels. Would an emergency from a cyberspace event function differently? Would any cyber-peculiar aspects change this model?

51. Is there a decision model for cyberspace for national incidents, something equivalent to the USAF taking over airspace for some length of time after 9/11? If not, what should one look like?

52. Is the U.S. populace receptive to the changes necessary to defend the nation that other countries have taken? If not, why not?

Additional Research Topics For Consideration

1. Cyber Force Structure Evaluation
2. Effective Talent Management in the Cyber Enterprise
3. Cyber Information Sharing and Understanding (Analytics Development)
4. Machine Learning (ML) in Defense of Networks
5. Deterrent Benefits of Offensive Cyber
6. Deterring Intellectual Theft
7. "Hired Guns" in Cyberspace
8. Convergence of Information Technologies (IT) and Operational Technologies (OT) where will it lead?
9. What does Defense Security Cooperation/Assistance in cyber mean?
10. How does the USCYBERCOM and its service components leverage International Affairs Specialist (IAS) and Foreign Area Officer (FAO) to expand partnerships?
11. Can/should Cyber Protection Forces be used to protect us critical infrastructure.
12. Integrated Effects in Cyberspace
13. Does DOD need an Intel organization dedicated to the Cyberspace Domain or a Federated approach?
14. Leveraging the College of Information of Cyberspace to educate Cyber Enterprise
15. International Norms in Cyberspace
16. A Strong Defense: the Key to Winning in Cyberspace?
17. Leveraging the Benefits of an Open Society in a Cyberspace/Information Operations (IO) Competition
18. Adversary/Cyber Threat Emulation Capacity Build
19. Advanced concepts that address DOTLMPF gaps for target sets in the plans (vulnerability analysis both DCO and OCO)
20. OCO and DCO Network Mapping Solution
21. What are Network Risk Forecasting Models
22. How does USCYBERCOM ensure it has the right people, skills, and capabilities now and in the future?
23. Architecting a new CIKR infrastructure that is more secure (to include capability development and policy)
24. Speeding Up the Acquisition Life Cycle for the Cyber Domain
25. Accelerating/Delegating the Approval Process Cyber Operations
26. Ease of Technology Enabled Communications impact on DOD
27. The Next Response to a Sony Pictures attack

Red –Topics likely to reach Secret

Additional Information

Student Researcher - Identification as a researcher does not necessarily imply financial sponsorship by US CYBERCOM, although an existing agreement with the National Defense University allows for limited funding for research.

Topic Sponsor – person within the US CYBERCOM assigned to provide feedback on a selected topic throughout the research period (Typically an academic year).

Topic Out brief – There are opportunities to brief topic research to Senior leaders within the cyber enterprise. Coordinated through the topic sponsor.

Topic Classification - The research is typically unclassified, but US CYBERCOM does accept support classified research efforts.

Assignment opportunities – Occasionally military and government civilian students who have gained an an in-depth understanding of a US CYBERCOM challenge and methods of addressing those issues can be outplaced in to a USCYBERCOM billet or one of it's Cyber components.

Briefings and/or other products from the research activity such as computer code or empirical models will be provided to the topic sponsor as appropriate.

We estimate a typical research report cost avoidance averaging over $100,000 per thesis.

United States Cyber Command
9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Completed research can be found at
uscybercom.mil (CAC Enabled)

For additional information please contact:
Ms. Shannen Parker - sgpark2@cybercom.mil
Lt Col Carlos Alford - clalfor@cybercom.mil