USCYBERCOM

2018 Cyberspace Strategy Symposium Proceedings

Preface

US Cyber Command hosted its inaugural Cyberspace Strategy Symposium at National Defense University on February 15, 2018. This day-long event showcased thought leaders from the Command and its partners inside and outside government pondering the challenges ahead for cyberspace operations. The Symposium's four panels and keynote addresses discussed current and likely issues, and debated USCYBERCOM's strategy and operations in a collective effort to improve operational outcomes. We believe the proceedings herein shed insight on the Symposium's central question: "What are the foundational organizing principles we need to operate more effectively in cyberspace?" The workshop's audience felt inspired to think creatively about USCYBERCOM's potential answers to this question, and I encourage readers of this publication to do likewise.

General Paul M. Nakasone
CDR USCYBERCOM

PANEL 1 – Cyber and the Information Environment

Discussion

The challenges of integrating cyberspace and information operations (IO) are not new, but over the last several years our adversaries have been aggressive and innovative, using a range of tools in cyberspace. It has been difficult for DOD to respond effectively. Adversaries are now employing IO and operating continuously short of armed conflict. They do not see a distinction between cyber and IO, and understand the importance of connectivity, content, and cognition. The United States government has traditionally sub-divided its IO concepts and activities, and has not adapted to these fundamental changes. In addition, Cyberspace is moving away from its hitherto civil-society dominated governance model.

Synchronizing and coordinating information-related capabilities together in a coherent strategy is piecemeal and limited today. Our adversaries, by contrast, are in a persistent state of competition, conducting influence operations to gain an advantage over us. DOD must be imaginative, within the bounds of law, policy, and capabilities, in integrating IO and cyberspace capabilities to counter and contest our adversaries globally.

Issues for Further Exploration

1. The relationship between cyber, what was historically called command and control (C2) warfare (adversary focused), and influence operations (which are not just adversary focused), and how to integrate these capabilities.
2. Relevance of concepts like area of responsibility and red-blue-gray space to the cyberspace domain.
3. How cyber is a subset of information operations.
4. Assumptions about the battlespace. Adversaries do not see the distinctions we do and operate more effectively at scale using a full range of tools.

PANEL 2 – Speed and Agility for Defense and Offense

Discussion

Cyberspace engagements can occur almost instantaneously, simultaneously, globally, and continuously. Success in the domain requires a whole-of-government approach that aligns to the interconnected battlespace--a domain that does not recognize territorial borders, sovereign territory, or areas of hostility. The 2018 National Defense Strategy identified the need for the joint force to be agile to prevail in conflict and preserve peace through strength.

The discussion explored several ways to conceive of and increase agility in cyberspace:

(1) Organize intelligence processes and partner with the rest of the Defense Intelligence Enterprise to increase agility and operational impact.

(2) Approach cyberspace operations like traditional fire and maneuver tactics to gain the ability to react to contact.

(3) Execute cyberspace operations through mission command.

(4) Approach cyberspace as a maneuver domain.

Issues for Further Exploration

1. Rules of Engagement (ROE) for operational commanders to respond with latitude to enable action like in other domains, where orders are written based on understanding of terrain, how the enemy would move, and a scheme of maneuver is built accordingly. This would enable Commanders to react to contact, have fire control measures, know their causalities, and synchronize with commanders on left and right sides.
2. Enabling component commanders to organize their forces as needed to counter adversary action.
3. Understanding of the cyberspace domain to include human interaction that spans the entire spectrum from competition to conflict, and recognition that DOD is in continuous

engagement with adversaries, as distinct from a narrower view of the domain as one of vulnerabilities, threats, and focused technical actions to close vulnerabilities.

4. Adopting a maneuver mindset rather than a management and maintenance mindset.
5. The factor of "speed." Is speed a limiting factor because we are a democracy. Can the U.S. be faster than its adversaries in cyberspace? If not, what offsets are available?
6. How do we measure risk in cyberspace? Assessment of risk at the tactical level and providing timely and relevant information to operational commanders. A reporting process using a series of stop light charts does not constitute risk management.

PANEL 3 – Integrating Cyberspace Operations into the Joint Force

Discussion

For cyberspace operations to remain relevant and integral to combat power projection, they must not differ from the other warfighting domains in fires and maneuver. One of our early lessons emphasizes that we should identify, vet, validate, nominate, and approve cyber targets in the same manner as we do for conventional strikes. A level of comfort is growing among senior leaders and commanders based on operational experience. Education and expectation management are key as cyber forces and capabilities bring credible options. To deliver all-domain integrated effects synchronized in timing and tempo as required by combatant commanders, the Services must integrate the concepts of cyberspace operations into how they organize, train, and equip the force. The discussion surfaced examples from practitioners and operational commanders who applied known and familiar concepts and are seeking improvement to joint operations by asking, "What might we adjust?"

Issues for Further Exploration

1. Fully integrating cyberspace operations into combatant commander plans as well as existing boards, bureaus, cells, and workgroups used to plan and execute warfare.
2. The nature of cyberspace as convergence and the need to integrate horizontally and vertically in thought and action.
3. Integrating the new Integrated Planning Elements with existing JCCs. Capturing best practices and lessons learned from combatant commands and sharing across combatant commands to accelerate integration and normalize cyber planning and operations.
4. Maturing cyber processes to provide cyber options and capabilities at the timing and tempo needed by operational commanders.
5. Understanding how cyber effects play out downstream, to include second and third order effects, to help operational commanders understand risk (vulnerabilities and exposures) and gain confidence.

6. How modeling and simulation environments can generate data and achieve greater levels of confidence and trust in cyberspace Battle Damage Assessment (BDA).
7. A common, formalized process to provide integrated cyber capabilities to the Joint Force. Capabilities developed by one Service need to be interoperable with capabilities and components delivered by other Services to be usable by a force comprised of personnel from yet another Service.
8. A common testing construct and process for developers, engineers, and operational commanders to determine whether a cyber effect will work as expected, one that all Services and Combat Support Agencies could adopt to calculate the spread, size of impact, and reversibility of the effect.
9. Increasing speed and agility in the development and integration of cyber tools for current operations. Testing to ensure the cyber capability performs its expected function in the operational environment, and accepting a "good enough" level of testing to manage risk and achieve speed and agility. Adopting standards and investing in flexible technologies.
10. A DOD measurement construct for which capabilities/tools at what quantity should reside in the "armory" to ensure the cyber force is equipped and ready to support operational commanders.
11. A balanced approach to account for operational gain and loss (OGL) and intelligence gain and loss (IGL) when calculating risk.

PANEL 4 – Defend the Nation

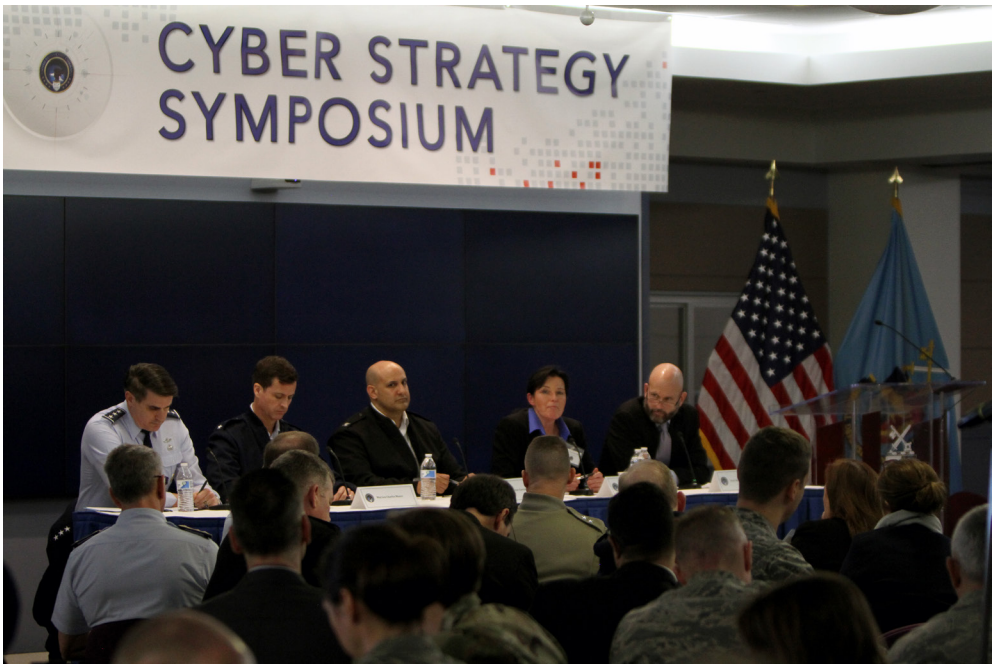
Discussion

This is one of the least developed mission areas and one in which there is little consensus on what it means to defend the nation and its interests in cyberspace, or on what role the Department of Defense should be for this mission. Some participants questioned whether DOD has a role in defending the nation in cyberspace. Others accepted that DOD has a role to play but debate its scope and purview, insisting that DOD should defend more than its own networks.

Issues for Further Exploration

1. Forging a DOD consensus on what its responsibility should be in defending critical infrastructure.
2. The terms and conditions of DOD's partnership with DHS, the States, critical infrastructure sector leads, and specific companies within critical infrastructure sectors. Seams between partners that inhibit planning, force sizing, capability development, and execution of military operations in support of partnership agreements.
3. Understanding public receptivity to, and tolerance of, military action in cyberspace as part of a yet-to-be-defined whole of society approach.
4. What constitutes a "significant" attack? Is a single attack significant? On the other hand, is "significance" in cyberspace a cumulative effect?
5. Clarifying the terms secure, protect, and defend to distinctly describe functions and advance the conversation. Secure is threat agnostic where everyone secures their systems and networks based on some set of standards (e.g., ISO 27001/27002, NIST guidelines). Protect is threat specific but passive where additional security may be added based on specific threats. Defend is a threat and capability focused activity designed to counter adversary strategy and capability.
6. The use of insurance to reduce critical infrastructure risks and inform DOD risk calculation and planning.

7. Ensuring operational realism and experience inform policy.
8. Is there a threshold of support that DOD should be expected to provide when a state or other sophisticated adversary attacks our critical information? When is it appropriate for industry and States to call on DOD for support? The value of "standing" Defense Support of Civil Authorities (DSCA) to shorten the decision cycle and make requests routine.
9. Federal Government barriers based on classification levels, sources and methods, and tear lines that hinder industry's ability to understand their environment and defend their networks.
10. The role of commercial intelligence processes that may outpace traditional military intelligence processes where DOD information is late-to-need. How DOD can disseminate information faster and at lower classification levels to increase its value and ability to share.
11. When do cybersecurity risks from businesses and private users take on national security implications?
12. How authorities that were issued prior to the growth of cyberspace may now increase risk of cyber attack.



Questions for Future Study and Analysis

USCYBERCOM compiled this list of 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. USCYBERCOM welcomes any products that respond to these topics.

MORNING KEYNOTES

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?

PANEL 1. 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?

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?

PANEL 2. Speed and Agility for Defense and Offense

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

KEYNOTE - 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?

PANEL 3. 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?

PANEL 4. 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?

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?

Notes

NSA Creative Imaging – 199197