COLUMBIA | SIPA
School of International and Public Affairs

CCSA
Cyber Conflict Studies Association

Tactical and Operational Dynamics of Cyber Conflict

AUTHORS: Trey Herr and Roberta Stempfley
SERIES EDITOR: Justin Key Canfil

Introduction

A recurring panel in the two-year history of the conference focuses on the tactical and operational dynamics of cyber conflict. The tactical and operational dynamics of cyber conflict deal with the mechanics of engagement, hewing away from issues like coercion and escalation towards the mechanics of capabilities development, employment, and maintenance. The operational focuses on the relationship between engagements and higher order processes like targeting, command & control, and training. The tactical emphasizes the minutiae of a single engagement, like the mechanics of a DNS reflection attack. Related panels covered Strategic Dynamics, as well as the Law, History, Intelligence processes, and Economics of cyber conflict.

The first conference in 2016 did as much to stoke discussion as organize the literature of cyber conflict. On tactical and operational dynamics, those assembled discussed the impact cyber operations would have on the tactical and operational levels of war as well as differences in the doctrinal development of different states and the relative offensive or defensive dominance of cyberspace. While there was mention of non-state actors, one of the biggest areas of expansion in the second year of the panel was to critically examine the role of the private sector in provisioning the infrastructure on which many of these engagements take place.

About the State of the Field Series

This article is part of the 2017 Cyber Conflict State of the Field (SOTF) paper series, under the auspices of the Cyber Conflict Studies Association and Columbia University's School of International and Public Affairs.

The conference, held annually since 2016, brings together experts from various academic disciplines, including political science, law, economics, and policy research, to define key questions and map the research frontier in the emerging field of cyber conflict studies. The conference is cumulative: each year builds upon past discussions. As a result, discussions have necessarily matured at different rates as new topics are added.

The papers in this series are meant to capture the findings of the 2017 conference. Together, the papers represent the conference attendees' understanding of the present state of the field in the academic study of cyber conflict.

Transition from 2016

In setting up the 2017 panel, we tried to bring together groups of questions that addressed similar topics while also focusing on the core of what tactics and operations would entail. We built on the topics above from the 2016 panel and modified them in expanding to the workshop outline for this year. The 2016 panel was broken into four sections: Cyber Power at the Tactical and Operational

Key Cross-Cutting Questions

- What aspects of tactical operations are physics, and cannot be changed, such as "speed of light" or "scale-free networks." What can we aspects change like "difficulty of attribution" or "offense dominance?" Indeed, what is the full set of all such aspects?

  How do these dynamics drive tactical and operational behavior i.e. effective defense requiring timely intelligence collection?

  How do these dynamics differ from the tactical and operational dynamics in other domains?

Levels, Legal and Ethical Considerations, Command & Control, and Organizational Considerations as well as discussion the formation of a cyber service. To adapt this organization, rather than create something new from whole cloth, we made two notable modifications to last year's organization. First, we reorganized some categories, breaking things down along more process-oriented lines so that concepts like Organizational Process didn't obscure meaningful internal distinctions. Second, we moved some literature to other panels; the discussion of both norms, a largely strategic issue, and law, self-evidently legal, fit better in the context of other panels.

Takeaways from 2017

This year's panel on tactical and operational dynamics built on discussion from the previous year, taking key questions and literature and adding to them. In the discussion, we saw three overarching themes which reflect in our comments about how to structure this area of cyber conflict research going forward.

1. There were a multitude of questions about the nature of cyberspace and the how the environment of cyber conflict could impact everything from building offensive capabilities to attributing attacks. This addresses a dicey line between disciplines as social scholars are asking about the nature of the computing and networked environment. This is a valuable area of work but one that emphasize careful literature review and resist the temptation to reinvent basic concepts like Benkler's articulation of the infrastructure, logical, and content layers of the internet or Clark's control point analysis.[1]
2. This panel and Strategic Dynamics still share some overlapping concerns. Some of this is due to the fluidity of operations in cyberspace. Much like the strategic corporal concept in insurgency, much of what can take place on a computer system can have outsize political impact. Ideas like anarchy, while theoretically intriguing, are largely structural in nature and thus beyond a reasonable discussion of tactical behaviors. In the interests of research coherence, more can be done to specify where concepts lie at the Strategic level vice the Operational or Tactical. We have endeavored to do so here.
3. There is a tremendously intimate mix of technically focused work out of computer science and operations research with political science, doctrinal analysis, and military science. The resulting amalgamation of methods, questions, and topics is difficult to hone into a coherent research area but the full diversity of work deserves our attention as it often talks to each other, if unknowingly. It would benefit future discussion on these topics if they more directly included computer science alongside the other represented disciplines. Friction will be inevitable but both instructive and valuable.

The rest of the paper covers the major questions and literature brought up in this year's discussion and closes with several recommendations for next year. Each section outlines some of the topics included in the category then proceeds to summarize the key questions, a combination of those carried forward from the 2016 panel and those generated for and during the discussion in 2017. Based on the discussion at the 2017 event and a recent paper on core readings in cyber conflict course syllabi, the following have emerged as three canonical works in cyber conflict:

- Herbert S. Lin, Kenneth W. Dam, and William A. Owens, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009)

- Thomas Rid. "Cyber War Will Not Take Place." Journal of Strategic Studies. 35:1 (2012): 5- 32. Or Rid, Thomas, 2013. *Cyberwar Will Not Take Place* (London: Hurst and Co.)
- Libicki, Martin C., *Cyberdeterrence and Cyberwar*, RAND Report, Santa Monica: Rand Corp., 2009

2017 State of the Field: Tactical and Operational Dynamics in Cyber Conflict

Structural Issues and Predicate Questions

Across the discussion there were repeated questions about the structure of cyberspace and conflict that weren't well addressed by other sections of the panel, for example, the relative offensive dominance of cyberspace. What ties the structural issues topic together is their consideration of the underlying rules and phenomena in which tactics and operations exist. While not a discrete section in the original design of the 2017 panel, these questions cropped up repeatedly and deserve explicit treatment. Technical Foundations is split apart to emphasize the role that the computing and network environments play in enabling and constraining cyber operations.

- What new metaphors could be useful to describe the environment of cyber conflict? What are the advantages and disadvantages of these different approaches?
  - humanitarian intervention
  - insurgency/counter-insurgency
  - climate change
  - public health
- What advantages or disadvantages extend from using offense vs. defense as a metaphor in studying cyber conflict?
  - Will this be true in the next 5, 10, 15 years?

Structural Issues and Assumptions

- What would be included in a taxonomy of actors, threats, events, capabilities, and key processes for cyber conflict at the tactical and operational levels?
- How have scholars and/or practitioners differentiated and operationalized the varying levels of war in this research area?[2] What are the merits of different approaches?
- Is cyberspace offense dominant?[3] Will it remain so and what are the implications?
- How have scholars assessed that non-Western perspectives, especially Chinese and Russian, differ on the structure and fundamental behavior of cyberspace?[4]
  - How have the differences between these perspectives changed in the last decade?
  - Where is this understanding best applied in US defensive efforts? Technical foundations? Doctrine? Strategy?
- How have or could scholars evaluate the assumptions underlying these questions, to understand which might change and under what conditions that change might take place?
- What is the relationship between the structure of the environment of cyberspace and the structure of organizations which adapt or are created to operate within it?[5]
  - How is this relationship changing with new technology like cloud-computing and more accessible machine learning resources?

Technical Foundations

- Is cyberspace subject to basic physics or engineering rules scholars need to consider, common dynamics that can be agreed to?
  - How might certain versions of these rules better complement some metaphors describing cyberspace over others?
- Cyberspace is often fungible and can be shaped by the participants; what are the structure, roles, and varying strategies of engagement for these actors?
- How have scholars weighed or measured the competing interests of the private sector and the US Government?
  - Where have or could these interests align to present opportunities for leverage by one party or the other?

Techniques and Technology

What are the key technologies and techniques that underpin tactical and operational cyber conflict? This section covers the specific processes used to identify, develop, deploy, maintain, and defend against cyber capabilities. Attribution deals with the range of methods used to identify and trace cyber operations, including the norms around conducting and publicizing this attribution. Generating and Maintaining Capabilities looks how the tools and material of cyber conflict is born, lives, and dies. This is a particularly expansive set of topics but combined here to promote the idea of these processes and technology interacting in a combined lifecycle.

Attribution[6]

- Under what conditions is attribution hard or easy?[7]
  - What are the implications from this?
- How do actors distinguish between espionage and OPE?[8]
  - Under what circumstances are these distinctions useful, or not useful? And what are the implications?
- What is the role of the private sector in attribution vis a vis the state, particularly the US Government?
  - Does the state have primacy?
  - Are there underexplored benefits or costs to private sector attribution?[9]
- Are there different norms, rules of behavior, for attribution?
  - Do these norms differ between states and non-state actors?
- How many of these concepts are true now, only in this moment, vs. true for all time?
  - How could attribution change in the event of conflict e.g. between US and China in South China Sea?

Generating and Maintaining Capabilities

- What is necessary to generate a cyber capability?[10]
- What sort of offensive or defensive capabilities can be generated without advance preparation?[11]
- What knowledge and resources are required to create high levels of effect? What are barriers to entry?[12]
- What is the minimal amount of effort or resources for an organization to operate effectively?
  - How do the malware market and the behavior of non-state actors impact the generation of these capabilities by states?[13]
- How does the process to generate information or influence as an offensive cyber capability differ from the development of software?
  - What impact do these differences have on theorizing around either the process to generate capabilities or outcomes from that process?[14]
- What is necessary to sustain a cyber operation?[15]
- How can actors manage a stockpile/arsenal of capabilities in a way that differentiates between activities that need new engineering input and those that don't? [The Great Kitchen Analogy]
  - Like cooking—some things needed fresh, for some there are substitutes
  - UK and French use similar ingredients, but everyone prefers French
  - Key is that integration, not a black box → integration is where the human factor comes in
- What are our adversaries and allies learning from the US about the modularity in offensive capabilities and how does this learning advantage overall global stability?
- What distinguishes the generation of offensive or defensive cyber capabilities from their maintenance or regeneration?[16]
- What resources, skills, or incentives influence the process of code or exploit development, reuse or proliferation?[17]
  - How quickly do offensive cyber capabilities decay in value/utility?[18]
  - What is the relative importance of single vulnerabilities versus a chain of such flaws to techniques to discovery or exploit them?

- How do we define and categorize offensive capabilities in cyber conflict?[19]
- How can organizations engineer/employ cyber capabilities with consideration for proportionality and proliferation?[20]
- What assumptions about the process to develop or employ offensive capabilities in cyberspace will be voided or altered in a crisis vs. in peacetime?
- What characteristics define damage in cyberspace?[21]
  - Does a definition of damage include reversible effects? Can it be quantified?
- What would be included in a "strategic toolkit" for cyber conflict?

Doctrine

This section covers issues of force employment and doctrinal development. There is rich potential for comparative work to evaluate the relative development, overlap, and key distinctions between the cyber operations doctrine of major cyber powers. This is of particular value in distinguishing between Western conceptions of tactics and operations and those of other states like Russia and China in answering many of the questions posed above. As cyber evolves both as a domain for operations and a domain to be integrated to achieve national objectives, there is emerging opportunity to understand how and when cyber and other operating domains are best employed and aligned.

Force Employment

- What are prominent taxonomies for effects and capabilities in cyber conflict?[22]
  - What are advantages or disadvantages to each of these approaches?
  - What would a universal taxonomy for these effects and capabilities include? How would it be structured?
- How are cyber operations integrated with conventional military capabilities?[23]
  - How could they in future?[24]
  - How do these approaches vary between different national doctrine?[25]
- Should/does the central role of infrastructure providers and software vendors change our conception of what "warfighting" is?
- How do conventional military or cyber operations combine with information operations?[26]
- What is the relationship between tactical engagements and a campaign?[27]
- How does secrecy impact the development of doctrine for, and exercise of, offensive cyber operations?[28]
- How do researchers theorize about intermediaries or vendors, e.g. Amazon, as a combatant?
  - Are vendors more immediately in the 'line of fire' on offense or defense?
- What factors would influence the distribution of forces on the battlefield/what are the peculiarities of battlefield use?[29]
- What are the core differences in cyber operations doctrine between the major powers?[30]

Organizations and Process

Who are the organizations involved in cyber conflict? This covers much more than what might be found on the battlefield given an environment built, shaped, and provisioned by people—largely the private sector. Considering the interests and behavior of actors like Microsoft and Akamai is as important for many tactical and operational questions of conflict. This section also contains more specifically battlefield issues including aspects of how to design and execute a Command & Control apparatus for cyber conflict at the tactical and operational levels.

Process and Categorization Questions

- What are the advantages and disadvantages of different approaches to categorizing the actors in cyber conflict?[31]
  - What can be learned from these varying approaches?
- How do scholars differentiate between information infrastructure firms involved in specific sectors vs. those with cross-

cutting impact? What are the advantages or disadvantages of these approaches?
    - How do the interests of these actors differ?[32]
    - How do these differences have regulatory or governance significance?
- Where do the interests of infrastructure providers differ from those of combatants?
- What are the mechanics and effects of information sharing e.g. in the ISAC/ISAO model?[33]
    - Under what conditions does information provide value to organizations? How does this value manifest and why?
- What is the influence of the intelligence community/culture on assumptions, beliefs, and expectations around cyber operations?
- How do states share cyber capabilities, offensive or defensive?
    - Under what circumstances would they want to?
    - How would the incentives, or mechanics, of sharing capabilities change in crisis vs. in peacetime?

Command and Control (C2) Considerations

- How should authorization for cyber operations be structured? Offense? Defense?[34]
- Are command and control constructs for cyber operations the same as they are in physical operations?[35]
- How should planning and targeting for cyber operations be conducted?[36]
- How will states and other actors integrate autonomous and rapid, automated, systems into their C2 process?[37]
- What confidence levels or probabilities are necessary for decision-making by national authorities?[38]
- What models exist for coordination in C2 between the private sector and the state?
    - How might this influence offensive private sector activities in response to an attack?[39]
- What distinctions exist in theorizing over the C2 of cyber operations vs. the integration of cyber operations in C2 of existing military operations?

Training and Skills

What are the educational processes required to develop skilled cyber operators? The key questions here are still developing but important enough to merit a distinct sub-category. These topics address the workforce involved in conflict. Some of the questions can go on to inform other topics like managing organizations responsible for cyber operations, like looking at the overlap of skills required for offense and defense.

- Are the skills and organizational capabilities required for offense and defense different?[40]
    - To what extent? How and where are skills different?
- What is the minimum level of training or skillset necessary for an individual to operate on offense, on defense?

Summary & Recommendations

The conversation during the panel was wide-ranging. Specific questions on how a piece of malware might be built of proliferated quickly spiraled into the norms around attributing such software's use and how to distinguish between its various potential effects. There was a recurring theme of mixing what seemed to be strategic questions, issues of escalation and deterrence for instance, into the minutia of organizational process issues like authorizing cyber operations in the United States. There was also a repeated emphasis on highly securitized topics, perhaps owing political science playing a prominent role in the intellectual development of the panel and many in the room. There is a tremendous influence of technology on many of these questions and even more so the companies and individuals that develop and maintain it. Stemming from these observations, we make two recommendations for researchers generally and next year's State of the Field in particular.

Split Tactical and Operational Research into Separate but Related Camps

The content covered by this paper should be split into two research areas—Tactical and Operational Cyber Conflict. Tactical should encompass all those activities and questions dealing with the conduct of a single engagement or activity while operational grapples with the ramifications and complexity of multiple engagements linked together. Deploying cyber capabilities on a battlefield works as a good example. The higher order planning issues, for example the question of how to integrate these capabilities within the planning process for a maneuver unit and matching cyber effects with supporting or direct fires—these are operational questions. Questions looking at lower level issues like the performance characteristics of deploying this capability over the Bluetooth protocol vs. 802.11g or the potential rate of decay in the utility of the vulnerability the capability depends on, are questions at the tactical level. Tactical thus encompasses a larger portion of the direct technical questions and conceptually sits closer to the metal. Operational deals with a higher level of abstraction and includes organizational, process, and many doctrinal issues.

There is a potential organizing logic between strategic, operational, and tactical levels.

- *How do I build it?* → *Tactical*
- *How should I manage or employ it?* → *Operational*
- *Why should I build or use it?* → *Strategic*

Push Discussion Beyond the Battlefield

There is a major body of work to be done on the integration of cyber capabilities on the battlefield but these questions are not the whole or even most questions in tactical and operational cyber conflict. During the 2017 workshop, there was a recurring challenge to integrate private sector actors in the discussion as something more than a structural oddity. Cyber conflict as a broad and interdisciplinary area of research should not be limited to understanding how the military will behave in the "cybered" era. Cyberspace is a man-made collection of technologies and standards, highly mutable compared to sea or space, and conceptually more complex with the asymmetrical power yielded by such groups as the IETF and criminal groups distributing ransomware. To study these topics, we argue that the technology vendors, non-governmental organizations, and intermediaries like cloud computing providers need to be made a more explicit topic of study. To this end, we have explicitly captured this dimension in the questions above.

Change over Time

How might these dynamics change over time? For example, will additional automation and AI drive transformational changes in defense and offense (as the radio, airplane, and tank did)? Or will they lead to more incremental changes (such as the switch from fourth- to fifth-generation fighters)?

Further, the rapidly evolving nature of the technology and introduction of machine learning and AI will require continued focus on these questions as it is unclear how the dynamics will change across the tactical, operational and strategic dimensions.

The tactical and operational dynamics of cyber conflict remain under-studied and broadly misunderstood by much of mainstream academia. Dismissing these topics as too grounded in technological minutia is a mistake for the social sciences. There is ample ground here for work by younger faculty and graduate students. Cyberspace is man-made and conflict over its boundaries or to kinetic effects through it must take that into consideration.

Acknowledgements

The authors would like to thank JD and the Cyber Conflict Documentation Project for their support as well as Jay Healey and Karl Grindal for comments and feedback. Lastly, thank you to all of the participants of the 2017 State of the Field workshop on Tactical and Operational Dynamics of Cyber Conflict for their participation, input, and insight.

About the Authors

Trey Herr, Ph.D., is a postdoctoral fellow with the Belfer Center's Cyber Security Project at the Harvard Kennedy School.

Roberta Stempfley is the Director of the CERT Division at the Carnegie Mellon University Software Engineering Institute.

End Notes

1. www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1242&context=fclj & https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032124
2. Murat Balci et. al — "Defining Military Levels for Cyber Warfare by Using Components of Strategy/ Ends, Ways, and Means", *21st ICCRTS — C2 in a Complex Connected Battlespace*, www.researchgate.net/publication/307923231_Defining_Military_Levels_for_Cyber_Warfare_by_Using_Components_of_Strategy_Ends_Ways_and_Means; Trey Herr and Drew Herrick — "Understanding Military Cyber Operations", *Cyber Insecurity — Navigating the Next Information Age*, https://books.google.com/books?id=NAp7DQAAQBAJ&pg=PA13&source=gbs_toc_r&cad=3#v=onepage&q=herrick&f=false
3. Rebecca Slayton — "What is the Cyber Offense-Defense Balance? Conceptions, Causes and Assessment", International Security, www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00267
4. Timothy Thomas. Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts. The Journal of Slavic Military Studies. Vol 27 No 1. March 2014; Timothy Thomas. Russian IW and an Analysis of Dr. Igor Nikolaevich Panarin. InfowarCon. Nashville, Tennessee. April 2015; Sergei A. Medvedev. Offense-Defense Theory Analysis Of Russian Cyber Capability. Naval Postgraduate School. March 2015; JD Work. Russian cyber operations in the current strategic landscape. Cambridge Intelligence Seminar. May 2017; Ammilee A. Oliva. China: Paper Tiger in Cyberspace. School of Advanced Military Studies, United States Army Command and General Staff College. March 2012.
5. Milton Mueller et. al — "Internet Security and Networked Governance in International Relations", *International Studies Review*, http://onlinelibrary.wiley.com/doi/10.1111/misr.12024/abstract
6. Panayotis a. Yannakogeorgos. Strategies for Resolving the Cyber Attribution Challenge. Air Force Research Institute. May 2013; Wylie McDade. Attribution, Delayed Attribution and Covert Cyber-Attack. Naval Postgraduate School. June 2014; Eric F. Mejia . Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework. Strategic Studies Quarterly. January 2014; Jeff Wozniak and Samuel Liles. Political and Technical Roadblocks to Cyber Attack Attribution. IO Journal. Vol 1 Issue 1. April 2009; Brian Bartholomew & Juan Andres Guerrero-Saade. Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks. Virus Bulletin Conference. October 2016 ; Don Cohen & K. Narayanaswamy. Survey/Analysis of Levels I, II,, and III Attack Attribution Techniques. ARDA. December 2004.
7. Thomas Rid and Ben Buchanan — "Attributing Cyber Attacks", *Journal of Strategic Studies*, www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382
8. Gary D. Brown — "Spying and Fighting in Cyberspace: What is Which?" *Journal of National Security Law and Policy*, http://jnslp.com/2016/03/29/spying-fighting-cyberspace/; Aaron F. Brantly. Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace. Intelligence and National Security. September 2015; Ramberto A. Torruella, Jr. Determining Hostile Intent in Cyberspace. Joint Forces Quarterly. 4th Quarter 2014.
9. Office of Director of National Intelligence. Public - Private Analytic Exchange Program. Cyber Attribution Using Unclassified Data. September 2016. Unclassified.
10. Max Smeets — "Transitory Nature of Cyber Weapons", *Journal of Strategic Studies*, www.tandfonline.com/doi/abs/10.1080/01402390.2017.1288107
11. iSIGHT Partners. Rapid Botnet Acquisition Within the Russian Underground Marketplace. February 2010.
12. Dorothy Denning. Barriers to Entry: Are They Lower for Cyber Warfare. IO Journal. Vol 1 Issue 1. April 2009; Christos Siaterlis and Béla Genge. Cyber- Physical Testbeds. Communications of the Acm. Vol 57 No 6. JUNE 2014; Cormac Herley. The Plight of the Targeted Attacker in a World of Scale. Workshop on the Economics of Information Security. June 2010; Giancarlo Pellegrino, Christian Rossow, Fabrice J. Ryba, Thomas C. Schmidt,

Matthias Wählisch. Cashing Out the Great Cannon? On Browser-Based DDoS Attacks and Economics. USENIX Workshop on Offensive Technologies. August 2015.

13. Trey Herr — "Malware Counter-Proliferation and the Wassenaar Arrangement", *Proceedings of the 8th International Conference on Cyber Conflict*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711070; Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez. Stocktaking study of military cyber defence capabilities in the European Union. RAND. Unclassified (summary); George Danezis and Bettina, The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications. Workshop on the Economics of Information Security. June 2006.

14. Christopher W. Weimer. Forecasting Effects of Influence Operations: A Generative Social Science Methodology. Air University. March 2012.

15. Paul D. Williams. USAF Cyber Capability Development. Air Command and Staff College Air University. April 2009; Paul H. Orth. Measuring the Operational Readiness of an Air Force Network Warfare Squadron. Air University. June 2008.

16. Kristen Dennesen. Hide and Seek: How Threat Actors Respond in the Face of Public Exposure. SANS Cyber Threat Intelligence Summit. Alexandria, Virginia. 3-4 February 2016.

17. Lillian Ablon, Martin C. Libicki, Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data. RAND. 2014; Rainer Böhme. Vulnerability markets — What is the economic value of a zero-day exploit. 22C3. Berlin, Germany. 2005; Michael Sutton and Frank Nagle. Emerging Economic Models for Vulnerability Research. Workshop on the Economics of Information Security. June 2006; Charlie Miller. The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales. Workshop on the Economics of Information Security. Carnegie Mellon University. 7-8 June 2007; Stefan Frei,; Francisco Artes. International Vulnerability Purchase Program. NSS Labs. December 2013; Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. Given Enough Eyeballs, All Bugs Are Shallow? Revisiting Eric Raymond with Bug Bounty Programs. Workshop on the Economics of Information Security. UC Berkeley School of Law. Berkeley, CA. 13-14 June 2016; Art Manion. A Survey of Vulnerability Markets. FIRST Conference. Boston, MA. 26 June 2014; Abdullah M. Algarni, Yashwant K. Malaiya. Software Vulnerability Markets: Discoverers and Buyers. International Journal of Computer, Information Science and Engineering Vol:8 No:3, 2014; Sam Ransbotham, Sabyaschi Mitra, and Jon Ramsey. Are Markets for Vulnerabilities Effective? MIS Quarterly. Vol 36 Issue 1. 2012; Andy Ozment. Bug Auctions: Vulnerability Markets Reconsidered. Workshop on the Economics of Information Security. University of Minnesota. Minneapolis, MN. 13-14 May 2004; Trey Herr, Bruce Schneier, and Christopher Morris, "Taking Stock: Estimating Vulnerability Rediscovery" *Belfer Cyber Security Project*, www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

18. Ashish Arora, Ramayya Krishnan, Anand Nandkumar, Rahul Telang, and Yubao Yang, Impact of Vulnerability Disclosure and Patch Availability — An Empirical Analysis. Workshop on the Economics of Information Security. May 2004; Rainer Böhme. A Comparison of Market Approaches to Software Vulnerability Disclosure. In: Müller G. (eds) Emerging Trends in Information and Communication Security. Lecture Notes in Computer Science, vol 3995. Springer, Berlin, Heidelberg. 2006. Lillian Ablon and Andy Bogart, "Zero Days, Thousands of Nights" (Santa Monica, CA: The RAND Corporation, 2017); Trey Herr and Bruce Schneier, "Taking Stock: Estimating Vulnerability Rediscovery," Cyber Security Project Paper (Cambirdge, MA: Belfer Center, Harvard Kennedy School, May 2017),

19. Trey Herr, "PrEP: A Framework for Malware and Cyber Weapons", *Journal of Information Warfare*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2343798; Trey Herr and Amy Armbrust, "Milware: Identification and Implications of State Authored Malicious Software" *New Security Paradigms Workshop*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2569845; Anita DíAmico, Laurin Buchanan, John Goodall1 and Paul Walczak. Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships Between Cyber Assets, Missions and Users. Proceedings of the Conference on Information Warfare & Security. 2010; Vitaly Tsygichko: Cyber Weapons as a new means of Combat. Classification of Cyber Weapons. Cyberwar, Netwar and Revolution in Military Affairs. International School on Disarmament and Research on Conflicts. Trento. 2002; Dale Peterson. Offensive Cyber Weapons: Construction, Development, and Employment. Journal of Strategic Studies. February 2013; James Morris-King, Hasan Cam. Ecology-inspired cyber risk model for propagation of vulnerability exploitation in tactical edge. Military Communications Conference MILCOM 2015. 26-28 October 2015.

20. Bellovin, Steven M., Susan Landau, and Herbert S. Lin — "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications." *Journal of Cybersecurity*, https://papers.ssrn.com/abstract=2809463; Kehler, Robert, Herbert S. Lin, and Michael Sulmeyer — "Rules of Engagement for Cyberspace Operations", Journal of Cybersecurity, https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyx003/3058505/Rules-of-engagement-for-cyberspace-operations-a; Robert Fanelli and Gregory Conti. A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict. in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 24th International Conference on Cyber Conflict. NATO CCD COE. 2012

21. Gregory J. Kula. Assessing the Effects of Computer Network and Electronic Attack. Naval War College. May 2009; John Tokar. Assessing Operations: MOP and MOE Development. IO Journal. Vol 2 Issue 3. August 2010. Carrie Gray and Edwin Howard. IO MOE Development and Collection: A Paradigm Shift. IOSphere. Spring 2005; Shirazi, Reza. "Botnet takedown initiatives: A taxonomy and performance model." Technology Innovation Management Review. Vol 5 Issue 1. 2015;

Yacin Nadji, Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee. Beheading hydras: performing effective botnet takedowns. Proceedings of the ACM SIGSAC conference on Computer & communications security. 2013; Hongxu Yin, Rui Xiao, Fenfei Lv. Analysis of Causes and Actual Events on Electric Power Infrastructure Impacted by Cyber Attack. Journal of Power and Energy Engineering. 2015; Dave MacEslin. Methodology for Determining Electronic Warfare Joint Munitions Effectiveness Manual. IOSPhere. Spring 2006; L. Scott Johnson and Toni Whyte. Lessons to be Learned from a Recent Network Infrastructure Attack. IO Journal. Vol 1 Issue 2. September 2009; Larry W. Fortson, Jr. TOWARDS The Development of a Defensive Cyber Damage and Mission Impact Methodology. Air University. March 2007; Richard A. Martino. Leveraging Traditional Battle Damage Assessment Procedures to Measure Effects from a Computer Network Attack. Air Force Institute of Technology. June 2011; Daniel BILAR. On nth Order Attacks. NATO CCD COE. 2009; Deborah Bodeau, Richard Graubart. Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment. Mitre. Technical Report 130432. November 2013; Christian Rossow, Dennis Andriesse, Tillmann Werner, Brett Stone-Gross, Daniel Plohmann, Christian J. Dietrich, Herbert Bos. SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets. IEEE Symposium on Security and Privacy. 2013; Scott Musman, Aaron Temin, Mike Tanner, Dick Fox and Brian Pridemore. Evaluating the Impact of Cyber Attacks on Missions. Proceedings of the Conference on Information Warfare & Security. 2010.

22. Lin, Herbert S., Kenneth W. Dam, and William A. Owens, editors — *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, www.nap.edu/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities; Colin F. Jackson — "Information Is Not a Weapons System", *Journal of Strategic Studies*, www.tandfonline.com/doi/abs/10.1080/01402390.2016.1139496; National Security Agency. Computer Virus Infections: Is NSA Vulnerable? Cryptologic Quarterly. Declassified in February 2008; Robert Majoris. Cyber Warfare as an Operational Fire. Naval War College. March 2010; Exploitation of Blue Team SATCOM and MILSAT Assets for red Team Covert Exploitation and Back-Channel Communications. David Rohret and Jonathan Holston. Proceedings of the Conference on Information Warfare & Security. 2010; Christopher Bronk and Eneken Tikk-Ringas. The Cyber Attack on Saudi Aramco. Survival. Vol 55 No 2. April-May 2013; David A. Rickards. No Air: Cyber Dependency and the Doctrine Gap. Naval War Collge. March 2010; Marc Romanych. Objectives in the Information Environment. IOSphere. Winter 2006. Per Kjellns. The Role of Computer Network Exploration (Active Sigint) in Information Warfare. Military Technical Section of The Royal Swedish Academy of War Sciences. 8 May 2001.

23. Michael Klipstein and Michael Senft, "Cyber Support to Corps and Below: Digital Panacea or Pandora's Box?" *Small Wars Journal*, http://smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box; Christopher R. Eidman, Gregory Scott Green. Unconventional cyber warfare: cyber opportunities in unconventional warfare. Naval Postgraduate School. June 2014; Steven Zielechowski. The Commanding Officer's Perspective on Protecting Shipboard IT Networks. Naval Postgraduate School. September 2014

24. Drew Herrick and Trey Herr — "Combatting Complexity", *Working Paper*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2845709; Max Smeets — "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks", *Proceedings of the 9th International Conference on Cyber Conflict*, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2002%20Organisational%20Integration%20of%20Offensive%20Cyber%20Capabilities.pdf;

25. Booz Allen Hamilton. When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure. September 2016; Dan Fayutkin. Russian-Chechen Information Warfare 1994-2006. RUSI Journal. Vol 151 No 5. October 2006.

26. Martin Libicki — "The Convergence of Information Warfare", *Strategic Studies Quarterly*, www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf; Drew Herrick — "The social side of 'cyber power'? Social media and cyber operations", *Proceedings of the 8th International Conference on Cyber Conflict*, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2007%20The%20Social%20Side%20of%20'Cyber%20Power'.%20Social%20Media%20and%20Cyber%20Operations.pdf; Information Operations by the British in the War of 1812 During the Maryland Campaign. Defense Intelligence Journal. Vol 12 No 2. 2003; Jonathan Reed Winkler. Information Warfare in World War I. The Journal of Military History. Vol 73 No 3. July 2009; David Acosta. The Makara of Hizballah: Deception in the 2006 Summer War. Naval Postgraduate School. June 2007. Carl Anthony Wege. Hezbollah's Communication System: A Most Important Weapon. International Journal of Intelligence and CounterIntelligence. Vol 27 No 2. March 2014

27. Martin Libicki — "Second Acts in Cyberspace", *Journal of Cybersecurity*, https://academic.oup.com/cybersecurity/article/3/1/29/3056957/Second-acts-in-cyberspace

28. Lin, Herbert S. and Taylor Grossman. "The Practical Impact of Classification Regarding Offensive Cyber Operations," in eds. Richard Harrison and Trey Herr, *Cyber Insecurity: Navigating the Perils of the Next Information Age*

29. Brian Thompson and Richard Harang — "Identifying Key Cyber Physical Terrain", *International Workshop on Security and Privacy Analytics (IWSPA)*, https://arxiv.org/abs/1701.07331; J. W. Mickens and Brian Noble — "Analytical Models for Epidemics in Mobile Networks", *Third IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications*, https://experts.umich.edu/en/publications/analytical-models-for-

epidemics-in-mobile-networks; Douglas H. Dearth. Applying Maneuver Warfare to Infrastructure Protection. InfoWarCon. 1999; L. M. Marvel et. al "A Framework to Evaluate Cyber Agility", *Military Communications Conference*, MILCOM, http://ieeexplore.ieee.org/document/7357414/

30. Amos C. Fox and Andrew J. Rossow — "Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo–Ukrainian War", *The Institute of Land Warfare*, www.ausa.org/publications/making-sense-russian-hybrid-warfare-brief-assessment-russo%E2%80%93ukrainian-war; Keir Giles — *Handbook of Russian Information Warfare*, NATO Defense College, www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

31. See Executive Order 13636, Section 9

32. Laura DeNardis — *The Global War for Internet Governance*, Yale University Press, https://books.google.com/books?id=jfxfAgAAQBAJ&pg=PR7&source=gbs_selected_pages&cad=3#v=onepage&q&f=false

33. Jason Healey. Threat and Warning for the Financial Sector. InfoWarCon. 2002; JD Work. Understanding information sharing in cyber intelligence communities of practice: Evidence from collaborative analytic exchange. Intelligence and the Cyber Environment. Brunel University, Uxbridge. November 2014; Payton A. Flynn, Sr. Cybersecurity: Utilizing Fusion Centers to Protect State, Local, Tribal, and Territorial Entities Against Cyber Threats. Naval Postgraduate School. September 2016; Erick Mandt. On integrating cyber intelligence analysis and active cyber defense operations. Uitica College. 2015; Kenneth A. Minihan. Intelligence and Information Systems Security: Partners in Defensive Information Warfare. Defense Intelligence Journal. Vol 5 No 1. 1996; Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware. Workshop on the Economics of Information Security. June 2014; Alex Pinto. Data-Driven Threat Intelligence: Metrics on Indicator Dissemination and Sharing. SANS Cyber Threat Intelligence Summit. Alexandria, Virginia. 3-4 February 2016.

34. Chesney, Robert — "Military-Intelligence Convergence and the Law of the Title 10/ Title 50 Debate." *Journal of National Security Law and Policy*, http://jnslp.com/wp-content/uploads/2012/01/Military-Intelligence-Convergence-and-the-Law-of-the-Title-10Title-50-Debate.pdf; Harry M Friberg. U.S. Cyber Command Support To Geographic Combatant Commands. U.S. Army War College. February 2011; Joseph E. Sisson. Fleet Cyber Command/Tenth Fleet: Enabling Cyber Unity of Effort. March 2010; Richard Mesic, Myron Hura, Martin C. Libicki, Anthony M. Packard, Lynn M. Scott. Air Force Cyber Command (Provisional) Decision Support. RAND. 2010.

35. S. W. Stone — "Agility in decision-making for cyberspace operations," *Military Communications Conference MILCOM*, http://ieeexplore.ieee.org/document/7795294/; S.W. Stone — "Factors related to agility in allocating decision-making rights for cyberspace operations" *Diss. Robert Morris University*, http://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/54da5be5e4b0e9d26e577151/1423596517506/096.pdf; Daryl L. Caudle. Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers. Office of the Chairman of the Joint Chiefs of Staff. Strategic Plans and Policy (J5). October 2010; David M. Franklin. U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority. Naval War College. March 2010; Joseph H. Scherrer, William C Grund. A Cyberspace Command and Control Model. Air War College. August 2009; Bradley L. Pybmu. Application of US Special Operations Command Model to Department of Defense Cyberspace Force. United States Marine Corps Command and Staff College, Marine Corps University. 2009; Norman R. Howes, Michael Mezzino, John Sarkesain. On Cyber Warfare Command and Control Systems. Department of Defense, Command and Control Research Program. Command and Control Research and Technology Symposium. 2004; Norman R. Howes, et. al. Cyber Warfare Command and Control System Users Manual. Institute for Defense Analysis. July 2003; Russell J. Caldwell. Information Operations (IO) Organizational Design and Procedures. Naval Postgraduate School. November 2004.

36. Long, Austin - "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." *Journal of Cybersecurity*, www.researchgate.net/publication/313933131_A_cyber_SIOP_Operational_considerations_for_strategic_offensive_cyber_planning; Fredrick Okello, Richard Ayres, Patrice Bullock, Brahim Erhili, Bruce Harding, Allan Perdigao. Information Warfare: Planning the Campaign. Air Command & Staff College. April 1996; Steven J. Smart. Joint Targeting in Cyberspace. Air and Space Power Journal. Winter 2011.

37. iSIGHT Partners. Potential 'Dead Hand' C&C Architecture Suggested by Adversary Adaptation Following Failed Botnet Takedown Attempt. February 2010; JD Work. Autonomy & Conflict Management In Offensive & Defensive Cyber Engagement. InfowarCON. Nashville, Tennessee. 5-7 April 2016.

38. Peter R. Stephenson. Towards Improving Attribution Confidence in Cyber Attacks. Journal of Cyber Conflict Studies. Vol 1 Issue 1. September 2006; Rudolph "Reb" Butler, Dick Deckro, Jeff Weir. Using Decision Analysis to Increase Commanders Confidence for Employment of Computer Network Operations. IOSphere. Fall 2005; Lou Anne DeMattei. Developing A Strategic Warning Capability For Information Defense. Defense Intelligence Journal. Vol 7 No 2. 1998; D.M. Rock. Cyber Attack: The Department of Defense's Inability to Provide Cyber Indications and Warning. Marine Corps Command and Staff Coll. 7 February 2006; Marco Roscini. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. Texas International Law Journal Volume 50, Symposium Issue 2.

39. Frans Mulschlegel, Jim Christy. Corporate Vigilantism: Striking Back. InfoWarCon. 1999; Winn Schwartau, W. Hutchinson. Corporate Vigilantism and the Hostile Perimeter. InfoWarCon. 1999; Stewart Baker, Orin Kerr, and Eugene Volokh. "The Hackback Debate". Steptoe & Johnson LLP. 22 November 2012.

40. Christopher Paul, Isaac R. Porche III, Elliot Axelband. The Other Quiet Professionals. Lessons for Future Cyber Forces from the Evolution of Special Forces. RAND. 2014; Timothy Franz. The Cyber Warfare Professional. Air & Space Power Journal. Summer 2011; Zhang Jun-qi,KE Hong-fa,ZHU Ji-luck. Discussion on Core Competencies and Construction Elements of Cyberwarfare Forces. Journal of Ordnance Equipment Engineering. July 2015; Joel Hill. Transforming Intelligence Education to Support Information Operations. Defense Intelligence Journal. Vol 12 No 1. 2003; Lynn M. Scott, Raymond E. Conley, Richard Mesic, Edward OíConnell, Darren D. Medlin. Human Capital Management for the USAF Cyber Force. RAND. 2010.

The Cyber Conflict Studies Association (CCSA) promotes and leads international intellectual development efforts to advance the field of cyber conflict research. These activities include workshops that bring together professionals from industry, academia and government to discuss strategic issues surrounding cyber conflict and the publication of insightful research articles and position papers and books. CCSA also plays an important role in our national cyber-readiness strategy, serving as a resource for national security decision-makers and helping to frame and promote national cyber conflict policy. CCSA brings together the best and the brightest individuals in the field of cyber conflict study to further the goals of national security and the field of cyber.

This work was supported in part by the Minerva Research Initiative. The Minerva Research Initiative, administered jointly by the Office of Basic Research and the Office of Policy at the U.S. Department of Defense, supports social science research aimed at improving our basic understanding of security.

Funded in part by the Office Naval Research under the OSD Minerva program, grant number: N00014-17-1-2423.