CCSA
Cyber Conflict Studies Association

Exploring the Dimensions of Intelligence in Cyber Conflict

AUTHORS: Dr. Michael Warner and Steven Loleski
SERIES EDITOR: Justin Key Canfil

Introduction

Since its introduction last year, the State of the Field conference has featured a number of analytically distinct but overlapping panel topics addressing issues of concern to the cyber domain. In particular, the panel on Intelligence and Adversaries has addressed the centrality of intelligence to the cyber realm. This year our panel focused on the reciprocal relationship between cyber and intelligence in order to unpack the dynamics between them before more closely zooming in on strategic, operational, and tactical issues relevant to intelligence processes. Our discussion touched on issues covered by other panels namely those covering Strategic, Tactical and Operational dynamics, and Cyber Conflict History.

The inaugural conference last year helpfully laid out some important questions and gaps in the literature in each respective topic area. With respect to the Intelligence field, discussion focused on conceptual matters surrounding intelligence itself along with attribution of cyber attacks. This year there was an effort to build upon this foundation and move beyond a discussion of intelligence processes to explore the broader relationship between cyber and intelligence. In other words, how has the cyber domain impacted intelligence and in turn, how intelligence has affected the cyber realm. While both intelligence in cyber and cyber in intelligence are at work, there were no clear answers to these questions and much work remains to be done specifying these dynamics. Participants raised comparisons to intelligence history in order to better assess the continuities or evolution from the past.

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.

Big Takeaways from 2017

This year's Intelligence and Adversaries panel continued to develop discussions from last year but endeavoured to frame the topic in a broader context. There were a few overarching themes that were touched upon at various points throughout our panel discussion.

1. ***History matters:*** while popular conceptions of cyber intelligence may dwell on the novelty of this domain, history can inform our understanding of evolutionary changes and continuities. In particular, concerns about the intelligence process and production at the operational and tactical level have clear parallels to Cold War operations. Moreover, exploring the path dependence of the emergence of cyber security largely under the auspices of intelligence organizations has affected how we approach this domain.
2. ***Escalation or restraint?*** There were a number of open questions about the nature of intelligence operations in cyberspace and whether these are (or are perceived) as offensive or defensive in nature. However, there was a consensus that we need to move beyond viewing cyberspace as inherently offense or defense dominant and instead look at changing strategic circumstances that make offense or defensive operations more likely. Toward this end, many participants were aware that intelligence operations can be both defensive and offensive and were concerned with how to credibly signal intentions especially across different nation-states. There was some overlap with other panels that explored strategic, operational, and tactical dynamics exclusively.
3. ***Structuring the discussion:*** there is a tendency to look at the familiar intelligence lifecycle to show how cyber has or has not affected traditional intelligence processes. This year our panel attempted to situate the discussion in broader terms and to be aware of the reciprocal influences between cyber and intelligence along strategic, operational, and tactical levels. However, these levels were not always easy to analytically separate in discussion.

2017 State of the Field: Intelligence and Adversaries

As mentioned, we had structured our discussion first to highlight the nature of cyber intelligence by encouraging participants to think about the mutually entangling dynamics between its constituent parts.

Intelligence in Cyber versus Cyber in Intelligence: It's both![1]

- To what extent does cyber emerge from the history of intelligence?[2]
- How analytically useful is the intelligence life cycle process in conceptualizing the cyber domain? What are some key differences?[3]
- What are the conceptual and organizational boundaries of intelligence and reconnaissance?
- To what extent are intelligence operations defensive or offensive in nature?[4]
- Who are the actors or communities producing intelligence? How do private or non-state actors figure into this discussion?
- What does it mean to collect intelligence through cyber?[5]
- How does intelligence affect cyber writ large or particular targets at the operational or tactical level?
- How do different nation-states approach the cyber domain and how can we establish credible measures of signalling intentions?[6]

Strategic-level considerations

How does cyberspace offer new opportunities for strategic intelligence forecasting? This section considers how cyberspace has affected decision-making by policymakers and in turn how it can be leveraged to provide strategic insight.

- How do decision-makers know what to expect in cyberspace?[7]
- How is cyberspace affecting the practice, organization, and legitimacy of intelligence?[8] How is that affecting citizens and enterprises?

- How is the cyber domain leveraged and used alongside conventional policy domains to achieve strategic objectives?
- How does cyberspace represent an opportunity for intelligence agencies to face strategic surprise a new way?[9]
- How can we leverage private firm reporting in documenting operational policy success or failure? What are the methodological challenges with doing so?
- To what extent will emerging technologies (Artificial Intelligence, machine learning, and quantum computing for example) destabilize or stabilize the cyber domain?

Operational-level considerations

This section covers the role of intelligence in operations and was largely discussed in the U.S. context. Further comparative national study of cyber operational and doctrinal mandates would enrich discussion.[10]

- How can we build and sustain capabilities that meet requisite strategic needs?
- How are cyber capabilities or cyber intelligence assets measured? What metrics can we employ to assess relative power in the cyber domain?
- How does organizational culture matter in the procurement and sustainment of cyber capabilities and intelligence assets?
- How are allies and adversaries planning and operating in cyberspace?[11]
- What is the relationship and role of intelligence in and during cyber operations? How has the intelligence community affected approaching cyber operations?
- To what extent does U.S. law and legal authorizations help or hinder U.S. cyber operations or intelligence gathering?[12]
- How can we think about the cost of cyber operations in achieving policy objectives?[13]

Tactical-level considerations

This section zoomed in to consider some tactical-level considerations on intelligence in cyberspace. Specifically, attribution and vulnerability disclosures seem to be drawing the most attention.

- Attribution! Who does what and to whom?[14]
- How does disclosing vulnerabilities affect intelligence collection?[15]
- Doctrine
  - What does "cyber" do to/for other intelligence disciplines?[16]
  - How are traditional intelligence methods being used in cyber?
  - Who will do all this, and how, and where? Will they know how?

Summary and Recommendations

The opening panel questions provoked a number of interesting comments and further questions pushing the discussion into other areas. One general observation was that there was not much in the way of sustained discussion or consensus about the distinctiveness of the cyber domain on intelligence. A participant in passing noted that the scale, speed, and risk of cyber operations have changed the dynamic but this remains to be explored in some depth. There may even be reasons to challenge these factors given that known cyber espionage campaigns have tended to be long-term operations and it is not altogether clear why or how cyber espionage has been more provocative than past espionage.

Second, a frequent tendency among participants was to conflate strategic, operational, and tactical issues in conversation or it may reflect some ambiguity with how these terms are precisely used with respect to the cyber domain. It may be helpful here to enter into conversation with other panels on strategic, operational, and tactical issues to develop common standards about how these terms are used in the cyber realm. Or this may be a broader issue related to the complexity of cyberspace itself as a domain with emergent properties.[17] For example, the Snowden disclosures were mentioned as an example where a single individual had the capacity to change the strategic conversation on

why and how the United States collects foreign intelligence.[18] It is not altogether clear what value added there is analytically by compartmentalizing and reifying the discussion into strategic, operational, and tactical dimensions unless warranted first and foremost by the research question under investigation. With these observations in mind, there are a few potential suggestions that may be worthwhile to consider for the future:

1. ***Encourage puzzle-driven research:*** the hallmark of most established scholarly disciplines is to enter into a puzzle- or problem-solving stage where interesting questions are addressed and middle-range theory develops. Instead of falling back to the comfort of comparing and contrasting cyber to the familiar intelligence process models, it would be useful to encourage a focus on different puzzles or testing middle-range theories. As cyber conflict history continues to be documented, this type of research has the potential to offer complementary case studies and also discuss the methodological challenges with cyber conflict research such as omitted or confounding variables. Also, this will encourage viewing cyber operations alongside more conventional covert operations that may have the benefit of specifying differences or the value added of cyber operations to outcomes. Another research gap identified above is the lack of attention to non-state group given the proliferation of capabilities open to small groups and individuals to conduct cyber espionage or targeted attacks.[19]

2. ***Developing research design and methods:*** social science disciplines in recent years have been moving to increased transparency surround research design and methods. As an emerging field, cyber conflict studies could benefit from a sustained focus on not only research agendas but also research designs and methods best suited to address the problems both unique to this domain and common with other conventional areas. Currently, most discussion of cyber conflict or intelligence remains focused on logical possibilities without sustained testing of those propositions. What needs to be done, following others,[20] is to develop datasets or cases to test and substantiate these claims. This has the potential to move discussion beyond whether cyberspace was inherently offense or defense dominant, which many participants agreed, was becoming exhausted. Having said that, it should be noted that single-case studies combined supplemented with other methods offers great potential value in generating new theoretical insights but also offer rigorous testing of causal mechanisms through within case observations.[21] Case studies may be all the more important in cyber conflict studies given the apparent but not insurmountable methodological problems of developing reliable datasets. Citizen Lab's seminal *Tracking GhostNet* investigation stands out as an example of multi-method work on a single case that yielded considerable insights on the nature of a particular cyber espionage operation.[22]

3. ***Encourage cross-pollination of panels:*** while the stand-alone panels have produced rich discussions in their own right, some observers noticed that certain topics like offense/defense balance were talked about simultaneously with the risk of certain groups talking past each other instead of with each other. It would be useful to encourage related panels to get together where certain issues that seem at odds could potentially be reconciled in a wider cyber operations frame of reference. For example, one observation during our panel was that it was difficult to separate where intelligence ends and an operation begins. As others have noted it quickly becomes clear that discussion bleeds into other panel topics where cyber operations leads to talk about norms and law for instance. Going back to the first suggestion, something to consider more further into the future as the State of the Field develops around common themes and literatures is to encourage paper submissions on cyber conflict writ large and for conference organizers to develop panels based on submissions from the field.

About the Authors

Dr. Michael Warner is the command historian of US Cyber Command and an adjunct faculty member at American University and Johns Hopkins University.

Steven Loleski is a Ph.D. Candidate in the Department of Political Science at the University of Toronto.

End Notes

1. Michael Warner, "Intelligence in Cyber—and Cyber in Intelligence," in *Understanding Cyber Conflict: Fourteen Analogies*, ed. George Perkovich and Ariel E. Levite (Georgetown University Press, 2017).
2. Gordon Corera, *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage*, 1 edition (New York: Pegasus Books, 2016); Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016); Craig Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (George Mason University, 2016), http://search.proquest.com/docview/1864633371/.
3. Jon R. Lindsay, "Cyber Espionage," in *Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford University Press, forthcoming 2018).
4. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April 3, 2015): 316–48; Gary Brown, "Economic Espionage: Spying and Fighting in Cyberspace: What Is Which?," *J. Nat'l Security L. & Pol'y* 8 (2016): 621–621; Aaron F. Brantly, "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace," *Intelligence and National Security* 31, no. 5 (July 28, 2016): 674–85, https://doi.org/10.1080/02684527.2015.1077620; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (January 1, 2017): 72–109.
5. Intelligence and National Security Alliance (INSA), "Cyber Intelligence: Setting the Landscape For An Emerging Discipline" (Intelligence and National Security Alliance (INSA), 2011), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_CyberIntel_WP.pdf.
6. Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Tai Ming. Cheung, Derek S. Reveron, and Jon R. Lindsay ([S.l.]: Oxford University Press, 2015), 1–28; Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services* (European Council on Foreign Relations, 2016), http://www.ecfr.eu/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_(WEB_AND_PRINT)_2.pdf.
7. Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*, First Edition first Printing edition (Athens, GA: University of Georgia Press, 2016).
8. Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Press, 2016); Jennifer Stisa Granick, *American Spies: Modern Surveillance, Why You Should Care, and What to Do about It* (Cambridge, United Kingdom: Cambridge University Press, 2017).
9. Richard K. Betts, *Enemies of Intelligence : Knowledge and Power in American National Security* (New York: Columbia University Press, 2007); Daniel Byman, "Strategic Surprise and the September 11 Attacks," *Annual Review of Political Science* 8 (2005): 145–70.
10. "Cybersecurity and Cyberwarfare: National Doctrine and Organization," accessed March 27, 2018, http://stefanomele.it/news/dettaglio.asp?id=275.
11. Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 19–28.
12. Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harv. Nat'l Sec. J.* 3 (2011): 85.
13. Slayton, "What Is the Cyber Offense-Defense Balance?"
14. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37.
15. Jason Healey, "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers," JIA SIPA, November 1, 2016, https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process.
16. Michael Warner, "Reflections on Technology and Intelligence Systems," *Intelligence and National Security* 27, no. 1 (February 2012): 133–53; Mark M. Lowenthal and Robert M. Clark, eds., *The Five Disciplines of Intelligence Collection*, 1 edition (CQ Press, 2015).

17. Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997).
18. "Presidential Policy Directive -- Signals Intelligence Activities," whitehouse.gov, January 17, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
19. Cortney Weinbaum, Steven Berner, and Bruce McClintock, "SIGINT for Anyone," Product Page, 2017, https://www.rand.org/pubs/perspectives/PE273.html; Marcos Degaut, "Spies and Policymakers: Intelligence in the Information Age," *Intelligence and National Security* 31, no. 4 (June 6, 2016): 509–31; Ronald J. Deibert et al., "Tracking Ghostnet: Investigating a Cyber Espionage Network," 2009.
20. Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace*, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013); Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (July 2013): 365–404.
21. Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005); Wiener, "Penetrate, Exploit, Disrupt, Destroy."
22. Deibert et al., "Tracking Ghostnet."

Bibliography

Betts, Richard K. *Enemies of Intelligence : Knowledge and Power in American National Security*. New York: Columbia University Press, 2007. http://www.loc.gov/catdir/toc/ecip0710/2007003937.html.

Brantly, Aaron F. "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace." *Intelligence and National Security* 31, no. 5 (July 28, 2016): 674–85. https://doi.org/10.1080/02684527.2015.1077620.

Brantly, Aaron Franklin. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. First Edition first Printing edition. Athens, GA: University of Georgia Press, 2016.

Brown, Gary. "Economic Espionage: Spying and Fighting in Cyberspace: What Is Which?" *J. Nat'l Security L. & Pol'y* 8 (2016): 621–621.

Byman, Daniel. "Strategic Surprise and the September 11 Attacks." *Annual Review of Political Science* 8 (2005): 145–70. https://doi.org/10.1146/annurev.polisci.8.082103.104927.

Corera, Gordon. *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage*. 1 edition. New York: Pegasus Books, 2016.

"Cybersecurity and Cyberwarfare: National Doctrine and Organization." Accessed March 27, 2018. http://stefanomele.it/news/dettaglio.asp?id=275.

Degaut, Marcos. "Spies and Policymakers: Intelligence in the Information Age." *Intelligence and National Security* 31, no. 4 (June 6, 2016): 509–31. https://doi.org/10.1080/02684527.2015.1017931.

Deibert, Ronald J., Rafal Rohozinski, A. Manchanda, Nart Villeneuve, and G. M. F. Walton. "Tracking Ghostnet: Investigating a Cyber Espionage Network," 2009.

Galeotti, Mark. *Putin's Hydra: Inside Russia's Intelligence Services*. European Council on Foreign Relations, 2016. http://www.ecfr.eu/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_(WEB_AND_PRINT)_2.pdf.

Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2 (April 3, 2015): 316–48. https://doi.org/10.1080/09636412.2015.1038188.

George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. MIT Press, 2005.

Granick, Jennifer Stisa. *American Spies: Modern Surveillance, Why You Should Care, and What to Do about It*. Cambridge, United Kingdom: Cambridge University Press, 2017.

Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.

———. "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers." JIA SIPA, November 1, 2016. https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process.

Intelligence and National Security Alliance (INSA). "Cyber Intelligence: Setting the Landscape For An Emerging Discipline." Intelligence and National Security Alliance (INSA), 2011. https://www.insaonline.org/wp-content/uploads/2017/04/INSA_CyberIntel_WP.pdf.

Jervis, Robert. *System Effects: Complexity in Political and Social Life*. Princeton, NJ: Princeton University Press, 1997.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Lindsay, Jon R. "Cyber Espionage." In *Oxford Handbook of Cyber Security*, edited by Paul Cornish. Oxford University Press, 2018.

———. "Introduction—China and Cybersecurity: Controversy and Context." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Tai Ming. Cheung, Derek S. Reveron, and Jon R. Lindsay, 1–28. [S.l.]: Oxford University Press, 2015. http://myaccess.library.utoronto.ca/login?url=http://books.scholarsportal.info/viewdoc.html?id=/ebooks/ebooks3/oso/2015-04-27/1/9780190201265-Lindsay.

———. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (July 2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

Long, Austin. "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 19–28. https://doi.org/10.1093/cybsec/tyw016.

Lowenthal, Mark M., and Robert M. Clark, eds. *The Five Disciplines of Intelligence Collection*. 1 edition. CQ Press, 2015.

"Presidential Policy Directive—Signals Intelligence Activities." whitehouse.gov, January 17, 2014. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (January 1, 2017): 72–109. https://doi.org/10.1162/ISEC_a_00267.

Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harv. Nat'l Sec. J.* 3 (2011): 85.

Warner, Michael. "Intelligence in Cyber—and Cyber in Intelligence." In *Understanding Cyber Conflict: Fourteen Analogies*, edited by George Perkovich and Ariel E. Levite. Georgetown University Press, 2017.

———. "Reflections on Technology and Intelligence Systems." *Intelligence and National Security* 27, no. 1 (February 2012): 133–53. https://doi.org/10.1080/02684527.2012.621604.

Weinbaum, Cortney, Steven Berner, and Bruce McClintock. "SIGINT for Anyone." Product Page, 2017. https://www.rand.org/pubs/perspectives/PE273.html.

Wiener, Craig. "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation." George Mason University, 2016. http://search.proquest.com/docview/1864633371/.

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.