COLUMBIA | SIPA
School of International and Public Affairs

CCSA
Cyber Conflict Studies Association

Cyber Conflict History

AUTHORS: Max Smeets and Jason Healey[1]
SERIES EDITOR: Justin Key Canfil EXECUTIVE EDITOR: Jason Healey

Introduction

The study of cyber history can provide insight into the often complex and obscure dynamics of cyber conflict. An exclusive focus on the present unnecessarily handicaps efforts to understand, categorize and qualify past behavior. Cyber history provides a storehouse of information on past cyber activity, including case studies and datasets that can fuel the formulation of theories and testable hypotheses. In addition to serving as a laboratory—however imperfect—to explain cyber behavior, the study of cyber history also helps academics, policy makers, and practitioners to interpret ongoing developments. To understand why a cyberattack—like the 2016 Democratic National Committee (DNC) email hack[2]—occurred, it is necessary to examine the historical context in light of present conditions. Was the targeting of the DNC espionage, an escalatory attack or criminal behavior? Was it a continuation of long-standing practices? Have similar methods been utilized in the past? Why did the attacker conduct this activity? A relatively recent history often suffices to explain key cyber conflict events and trends, but in some cases, it is necessary to delve further back in time to fully understand the underlying causes.

There is simultaneously too much and not enough cyber history. The secrecy surrounding government organizations and their capabilities as well as the anonymity of attackers complicate the documentation of cyber history. Moreover, the recent and rapid growth of the field means the subject has yet to receive adequate attention from professional historians.[3] Vast amounts of raw data, case study reports, and other documents still await analysis and therefore leave much research left to be undertaken.

It is hardly surprising that SOTF devoted a panel to cyber history, given its importance and the work that remains to be done. SOTF first included a cyber history panel, with Jason Healey moderating, in 2016. Karl Grindal summarized the key views of the panelists and provided a comprehensive overview of canonical works in the field.[4] The 2017 panel built on that of the previous year with only minor changes. The

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.

table below provides an overview of the topics on the agenda at the State of the Field conferences in 2016 and 2017.

	TOPICS	
	STATE OF THE FIELD 2016	STATE OF THE FIELD 2017
I	Origins of the Cyber Domain	Conceptual History
II	Development of the Field	History of Cyber Conflict Discourse
III	Eras in Cyber Conflict History	Eras in Cyber Conflict History
IV	Organizational History	Organizational History
V	Operational History	Operational and Strategic History*
VI	History of Non-State Actors	

* On agenda but not discussed during workshop due to lack of time.

Major Takeaways from SOTF 2017

Discerning the continuities and discontinuities of cyber conflict formed the central and overarching theme of the panel. Although the two perspectives were not explicitly compared, elements of each came up throughout the discussion. Participants discussed several "turning" and "tipping" points throughout cyber history as potential points of discontinuity. These tipping points also offer potential qualitative shifts and likely differ across countries/regions, making periodization complex and inherently spatially bounded. Complicating matters further, cyber events (e.g., the Morris Worm, Stuxnet, and Operation Orchard) and non-cyber events (e.g., the Oklahoma City Bombing, the Asian Financial Crisis, and the November 2015 Paris terrorist attacks) alike were identified as potential roots of decisive change in this field.[5] But beyond the many spatial and temporal discontinuities identified were signs of remarkable continuity in the nature of cyber conflict, including an ever-evolving relationship between "cyber" and "info" warfare.

I. Conceptual History

QUESTION(S):	GAP(S):
• How has our perception of cyber-related concepts changed? • How does conceptual ambiguity affect governance?	• The relationship between the prefix "cyber" and other terms (e.g., "info," "computer," etc.).

The workshop session started with a discussion on the historical semantics of cyber-related terms. The term "cyberspace" has long been attributed to William Gibson, who first used it in the 1982 short story "Burning Chrome" and again in his 1984 novel *Neuromancer*.[6] However, it has now been traced back to an earlier etymology. An article in a Norwegian art magazine suggests the term may have first appeared, without gaining currency, in a painting collage produced by Susanne Ussing and Carsten Hof between 1968–1970.[7] John Perry Barlow is credited with introducing "cyberspace" to political discourse in 1996.[8]

Regardless of its origins, the term has been interpreted in numerous ways and embodied a variety of meanings over the years. In assessing the history of cyber-related concepts,[9] panelists identified two primary questions:

- How has our understanding of cyber-related concepts changed?
- How does conceptual ambiguity affect governance?

Following the discussion, panelists made the key observation that it is only possible to understand the nature of cyberspace by assessing its pre-history. They referenced a brief history by several chief architects of the Internet on the technical foundation of the Advanced Research Projects Agency Network (ARPANET).[10] This account emphasizes the decentralized, trust-based nature of the project. The panelists also reiterated a point raised in 2016, that the prefix "cyber" is still often conflated with other terms, such as "info," "computer," or "the Internet." This ongoing conflation and ambiguity of terms hinders policy efforts to establish "rules of the road."

One participant noted the importance of understanding how "cyber" became a military domain, guiding our organizational and strategic thinking. In 2011, the U.S. military forces officially expanded the traditional

domains of warfare—air, sea, land, and space—to include cyber.[11] A number of countries have subsequently adopted a similar approach, and in 2016 NATO also officially declared cyberspace a warfare domain.[12] Both the historical origins and the implications of conceptualizing cyberspace in this manner remain ill understood.

Finally, participants noted that the conceptualization of cyberspace and its relevant terminology varies across countries. For example, a report from the East-West Institute states, "Unlike Americans, Russians saw cybersecurity as an inextricable part of a larger discussion on information security."[13] Regional differences are also evident in the interpretation of "cyber sovereignty," which describes a government's goal of exercising control over cyber activities within its own borders.[14]

II. History of Cyber Conflict Discourse

QUESTION(S):	GAP(S):
• How has the discourse surrounding cyber conflict (and the cyber threat) developed over time?	• U.S.-centric. • Limited group of actors analyzed.

The study of discourse and narratives is becoming increasingly important to the field of conflict resolution. Scholars have been analyzing the cyber security discourse since the early 2000s.[15] Myriam Dunn Cavelty makes a compelling and comprehensive argument that cyber threats have been inflated by numerous policymakers.[16] Limiting his scope to the United States, Ralf Bendrath reaches a similar conclusion: "there is no link at all between the cyber threat perception and the real world."[17] Although the field has evolved around the literature on securitization, scholars have also addressed the consequences of cyber threat inflation. Thomas Rid and Robert M. Lee contend that "cyber-angst" is damaging and self-serving and that a more nuanced debate is needed.[18]

Workshop participants addressed a key gap in the current academic discussion on cyber discourse: the lack of scholarship into how cyber threat assessment and general threat assessment affect each other. They highlighted the November 2015 Paris attacks as a potentially interesting case warranting analysis. Historically, the primary focus of cyber conflict has centered on attacks originating in Russia and China. The 2015 terrorist attacks in Paris, while not cyber conflict, catapulted "cyber terrorism" back into focus as a key threat to the general public.

In addition, participants noted that the ongoing discussion of the nature of cyber conflict—often post-cyber incident—takes place in a number of different forums. They pointed out that many excellent insights on recent cyber activity have appeared on Twitter instead of in the mainstream media. The research community needs to think carefully about how best to capture these views to ensure that they will not be lost to reports published in future case studies.

Finally, participants noted that the tendency to attach the prefix "cyber" to other terms, though ongoing, may slow or cease in the future. As one participant observed, we no longer talk about the "digital economy"—it's just the "economy." "Cyber warfare" may someday mirror this trend; "cyber" will come to seem inherent to, and implicit in, "warfare."

III. Eras in Cyber Conflict History

QUESTION(S):	GAP(S):
• How can we divide cyber conflict history into eras? • Which incidents or moments serve as transition points between these eras? • How did institutions develop around cyber conflict in the early era? • How has the balance changed between military operations and intelligence as a matter of doctrine, organization, and practice? • How has cyber conflict history already been divided into "eras"?	• What unique technical and political attributes are linked to these eras? • How do different levels of granularity overlay when we outline the history of cyber conflict?

The third topic on the agenda was "Eras in Cyber Conflict History," with "eras" viewed as frameworks that we impose over events to make sense of them. In his "pre-history" of cyber security, Michael Warner argues that the U.S. government's insights can be categorized into four phases:

- Computers can spill sensitive data and must be guarded (1960s)
- Computers can be attacked, and data can be stolen (1970s)
- We can build computer attacks into military arsenals (1980s and 1990s)
- Others might do the same to us—and perhaps already have (1990s)[19]

Healey, by contrast, identifies three phases of cyber conflict history: realization (1980s), takeoff (1990s–), and militarization (2003–).[20] Awareness of the potential of cyber conflict grew through various events in the 1980s and 1990s, including the Morris Worm (1988), the Wank Worm (1989), the Cuckoo's Egg (1989), Michelangelo (1992), Eligible Receiver (1997), and Solar Sunrise (1998). Post-2000, several events, including the Code Red Worm (2001), the SQL Slammer Worm (2003), JSF espionage (2009), and Stuxnet (2010), increased the sense that targeted cyber activity would only intensify.[21]

Workshop participants echoed two points from earlier cyber history discussions: first, that non-cyber events have, at times, been instrumental in shaping cyber policy. For example, the murder of 168 and injuring of hundreds more in the 1995 Oklahoma City bombing likely impacted the United States' formal response to cyber threats. Following the attack, the Clinton administration formed the President's Commission on Critical Infrastructure Protection, which released a report stressing the need to implement new measures around cyber security.[22] Second, that periodization differs significantly across regions. For example, as was noted, Chinese experts published several articles in the mid-1990s on the United States' growing interest in information warfare.[23] The Chinese also likely learned important lessons from Operation Orchard, Israel's 2007 use of electronic warfare to neutralize Syrian radar systems, facilitating an airstrike on a suspected nuclear reactor.

In the Middle East, rapid change occurred from 2009–2012, when Stuxnet was revealed and popular uprisings partially fueled by online mobilization hit multiple autocratic regimes. The events of the Arab Spring, though often forgotten, are arguably as relevant as Stuxnet to the course of cyber policy in this region. To quell protests, governments across the Arab world severely tightened Internet controls, arrested bloggers, stole passwords for social media accounts, and in several countries (Egypt, Libya, and Syria), even attempted to shut down the Internet completely. The perspective of many autocratic regimes in the region was that the cyber threat was coming from multiple vectors simultaneously.[24]

While these examples of periodization in China and the Middle East are illuminating, participants noted that a broad overview of which events were essential for different countries or regions is still missing.

IV. Organizational History

QUESTION(S):	GAP(S):
• How have legislation, rules, and doctrines evolved to address cyber threats? • How have major cyber incidents impacted organizational policies or structures? • Have doctrinal and organizational developments abroad been secondary or primary factors for domestic organizational change? • How have organizations adopted and incorporated offensive cyber capabilities? • How can non-state actors help to establish and cascade cyber norms?	• Weighted toward institutions that have either defended or threatened the United States. • The impact and evolution of non-governmental organizations is underexplored. • Interstate cooperation (particularly on offensive).

Scholarly discussion of organizational responses to cyber conflict has taken place on several levels. Most research has focused on the relationship *between* the

public and private sectors in *defending* cyberspace. The specific conditions under which information should be shared and the extent to which non-voluntary standards should guide the public-private relationship form a central consideration within organizational responses.[25]

Workshop participants identified the high level of secrecy as a barrier to discussion about how the links *within* government relate to the conduct of *offensive* operations.[26] Future research is necessary on the relationship between offensive intelligence operations and offensive military operations—or what the U.S. military calls Computer Network Exploitation (CNE) and Computer Network Attack (CNA).

Another often-overlooked area of study within the field is the role of informal "trust networks." Milton Mueller writes, "there is a strong and persistent tension between state sovereignty, which is territorially bounded, and the nonterritorial space for social interaction created by networked computers."[27] This tension, and the non-nation-centered arrangements that may follow from it, deserve further analysis.

From an organizational perspective, the intertwining of cyber warfare and information warfare has been critical to some governments while an anathema to others. Following the DNC hack, many experts have prioritized a reorientation toward countering information operations. As one participant observed, this focus is nothing new: "In the United States, there was a debate about it 20 years ago. Interestingly, the term 'cyber' was purposefully separate to make sure it becomes 'something' on its own; it showed that it went beyond psychological warfare. Yet, some now go down this road, which back then was seen as a dead end." The voluminous documentation on information warfare following the Kosovo War and the liberation of Kuwait in the 1990s supports this point, as does the outlining of the elements underlying "information warfare" in a 1976 paper by Boeing engineer Thomas P. Rona.

Finally, there remain open questions about how cyber conflict relates to issues of global order. Despite ongoing initiatives from the Global Commission on Cyberspace, it is unclear how we can embed cyber regimes into broader global stability. Note that even though the current reading lists include references on "cyber norms," several participants argued that it would be better to address that issue separately.

V. Operational and Strategic History

QUESTION(S):	GAP(S):
• How have operators detected, identified, responded to, and recovered from major cyber incidents? • Can current cyber defenders or policymakers draw any lessons from past operational incidents? • Is there fundamental continuity or discontinuity in cyber operations? • Which early works helped to shape strategic thinking on cyber conflict?	• Still lacking comprehensive case studies. • Analysis of incidents using historical datasets is still limited to a few scholars. • There is no clear sense of how pre-cyber operations link to current-day cyber activity.

There are many open questions when it comes to operational and strategic cyber history. Unfortunately, the discussion was cut short due to time limitations.

Concluding Remarks

As the panel discussion emphasized, cyber history is simultaneously characterized by "continuous change" as well as "turning points." While time constraints prevented participants from providing a comprehensive overview of the field, the identified gaps establish a natural starting point for discussion at the next SOTF. At the next workshop, it may be especially worthwhile to focus on the operational and strategic history of cyber conflict. This could include an overview of known cases that have received insufficient attention.

Important Works

Conceptual History: Meaning of Cyber(space)

PRIMARY READING

Cornish, Paul. (2015) Governing Cyberspace through Constructive Ambiguity. *Survival*, 57(3): 153-176.

Gibson, William. (1984) *Neuromancer*. London: Victor Gollancz.

Hayden, Michael. (2011) The Future of Things "Cyber." *Strategic Studies Quarterly*, 5(1): 3-7.

Rid, Thomas. (2016) *Rise of the Machines*. New York: W.W. Norton & Company.

Wolff, Josephine. (2016) What we Talk About when we Talk About Cybersecurity: Security in Internet Governance Debates. *Internet Policy Review*, 5(3).

SECONDARY READING

Betz, David and Tim Stevens. (2011) *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge.

Ebert, Hannes and Tim Maurer. (2013) Contested Cyberspace and Rising Powers. *Third World Quarterly*, 34(6): 1054-1074.

Giles, Keir and William Hagestad II. (2013) Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In *NATO CCD COE Publications*, K. Podins, J. Stinissen and M. Maybaum (eds.), 5th International Conference on Cyber Conflict.

Herrera, Geoffrey L. (2006) *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany: State University of New York Press.

Kello, Lucas. (2013) The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2): 7-40.

Maurer, Tim and Robert Morgus. (2014) Compilation of Existing Cybersecurity and Information Security Related Definitions. New America Foundation.

History of Cyber Conflict Discourse

PRIMARY READING

Bendrath, Ralph. (2003) The American Cyber-Angst and the Real World — Any Link? In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, R. Latham (ed.). New York: The New Press.

Dunn Cavelty, Myriam. (2008) *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*. Abingdon: Routledge.

Hansen, Lene and Helen Nissenbaum. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53: 1155-1175.

SECONDARY READING

Walt, Stephen M. (2010) Is the Cyber Threat Overblown? *Foreign Policy*, http://walt.foreignpolicy.com/posts/2010/03/30/ is_the_cyber_threat_overblown.

Eras in Cyber Conflict History

PRIMARY READING

Bamford, James. (2002) *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor Books.

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

Kahn, David. (1996) *The Codebreakers: The Story of Secret Writing*. New York: Scribner.

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

Rid, Thomas. (2016) *Rise of the Machines*. New York: W.W. Norton & Company.

SECONDARY READING

Aldrich, Richard. (2010) *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: Harper Collins.

Bamford, James. (1983) *The Puzzle Palace: A Report on America's Most Secret Agency*. New York: Penguin Books.

Harris, Shane. (2015) *@War: The Rise of the Military-Internet Complex*. New York: Houghton Mifflin Harcourt.

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

Warner, Michael. (2012) *Cybersecurity: A Pre-History. Intelligence and National Security*, 27(5): 781-799.

Yardley, Herbert O. (2004) *The American Black Chamber*. Annapolis: Naval Institute Press.

Organizational History

PRIMARY READING

Johnson, David R. and David G. Post. (1996) Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, 48b: 1367-1402.

Lessing, Lawrence. (1998) The Laws of Cyberspace. Working paper, Harvard Law School. https://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf.

Lipner, Steven B. (2015) The Birth and Death of the Orange Book. *IEEE Annals of the History of Computing*, 37(2): 19-31.

Maurer, Tim. (2011) Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security. Belfer Center, Discussion Paper #2011-11, Explorations in Cyber International Relations Discussion Paper Series.

Ruffini, Joseph. (1999) 609 IWS Chronological History. Department of the Air Force.

SECONDARY READING

Carr, Madeleine. (2016) Public-Private Partnerships in National Cyber-Security Strategies. *International Affairs*, 92(1): 43-62.

Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. (2014) Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, 20(2): 96-121.

DeNardis, Laura. (2015) The Internet Design Tension between Surveillance and Security. *IEEE Annals of the History of Computing*, 37(2): 72-83.

Finnemore, Martha and Duncan B. Hollis. (2016) Constructing Norms for Global Cybersecurity. *The American Journal of International Law*, 110(3): 425-479.

Hurwitz, Robert. (2014) The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests*, 36(5).

SECONDARY READING	Nye, Joseph. (2014) *The Regime Complex for Managing Global Cyber Activities*. Harvard Kennedy School Belfer Center. Available at http://belfercenter.hks.harvard.edu/files/global-cyber-final-web.pdf. Rosensweig, Paul. (2010) The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence. In National Research Council, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Available at sites.nationalacademies.org/cs/groups/cstbsite/ documents/webpage/cstb_059443.pdf. Yost, Jeffrey R. (2015) The Origin and Early History of the Computer Security Software Products Industry. *IEEE Annals of the History of Computing*, 37(2): 46-58.

History of Operational and Strategic Thinking

PRIMARY READING	Arquilla, John and David Ronfeldt. (2001) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: Rand Corporation. Buchanan, Ben and Michael Sulmeyer. (2016) Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity. Paper, Cyber Security Project. Harvard Kennedy School Belfer Center. Available at www.belfercenter.org/sites/default/files/legacy /files/hacking-chads.pdf. Denning, Dorothy E. (1998) *Information Warfare and Security*. New York: Addison-Wesley Professional. Harknett, Richard J. (1996) Information Warfare and Deterrence. *Parameters*, 26(Autumn): 93-107. Libicki, Martin C. (1995) What is Information Warfare? Strategic Forum, No. 28, Washington: National Defense Univ., Institute for National Strategic Studies. Lindsay, Jon. R. (2013) Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3): 365-404. Ottis, Rain. (2008) Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Proceedings of the 7th European Conference on Information Warfare, 163. Rattray, Gregory J. (2001) *Strategic Warfare in Cyberspace*. Boston: MIT Press. Schwartau, Winn. (1996) *Information Warfare: Second Edition*. New York: Thunder's Mouth Press. Zetter, Kim. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.
SECONDARY READING	Denning, Peter. (1990) *Computers Under Attack: Intruders, Worms, and Viruses*. New York: Addison-Wesley. Farwell, James P. and Rafal Rohozinski. (2011) Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*, 53(1): 23-40. Herzog, Stephen. (2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 4(2): 49-60. Hollis, David. (2011) Cyberwar Case Study: Georgia 2008. *Small Wars Journal*. Oder, Joseph E. (1994) Digitizing the Battlefield: The Army's First Step to Force XXI. *Army*: 36-42. Rid, Thomas. (2017) Disinformation: A Primer in Russian Active Measures and Influence Campaigns. Hearing before the Select Committee on Intelligence, United States Senate. Toffler, Alvin and Heidi Toffler. (1995) *War and Anti-War: Making Sense of Today's Global Chaos*. New York: Grand Central Publishing.

About the Authors

Dr. Max Smeets is a cybersecurity postdoctoral fellow at Stanford University Center for International Security and Cooperation (CISAC). He is also a non-resident cybersecurity policy fellow at New America, and Research Associate at the Centre for Technology & Global Affairs, University of Oxford.

Jason Healey is a Senior Research Scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict, competition and cooperation.

End Notes

1. The authors would like to thank Aaron Brantly and Karl Grindal for their helpful comments on earlier drafts of this report.
2. Thomas Rid, "How Russia Pulled Off the Biggest Election Hack in U.S. History," *Esquire*, (20 October 2016), retrieved from: www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/
3. As one participant noted, "Federal historians are a dying breed—they get cannibalized before something else [which directly impacts mission execution]."
4. Jason Healey and Karl Grindal, "The Cyber Conflict State of the Field Workshop Report 2016," The Cyber Conflict Studies Association.
5. The workshop participants, however disagreed on what "decisive change" would entail in this field.
6. William Gibson, Burning Chrome, *Omni*, 46 (1982, July); Gibson, *Neuromancer*, (London: Victor Gollancz, 1984)
7. Jacob Lillemose and Mathias Kryger, "The (Re)invention of Cyberspace," *Kunstritikk*, (24 August 2015), retrieved from: www.kunstkritikk.no/kommentar/the-reinvention-of-cyberspace/
8. John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, (1996), retrieved from: https://projects.eff.org/~barlow/Declaration-Final.html
9. Note that previous research efforts—e.g., Thomas Rid's *Rise of the Machines*—show that there is an (academic) market for this type of work.
10. Barry M. Leiner, Vincent G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review*, 39:5 (2009): 22–31. First published 1992
11. Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly*, 46 (2007): 58–61
12. Tomáš Minárik, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit," NATO Cooperative Cyber Defence Centre of Excellence, (21 July 2016), retrieved from: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html
13. Karl Frederick Rauscher, "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations," East-West Institute, (26 April 2011), retrieved from: www.eastwest.ngo/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations
14. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, (New York: W.W. Norton Company, 2015)
15. Helen Nissenbaum, "Hackers and the Contested Ontology of Cyberspace," *New Media & Society*, 6:2 (2004): 195–217; Nissenbaum, "Where Computer Security Meets National Security," *Ethics and Information Technology*, 7:2 (2005): 61–73; Rachel Yould, "Beyond the American Fortress: Understanding Homeland Security in the Information Age." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham (New York: The New Press, 2003); James Der Derian, "The Question of Information Technology in International Relations," *Millennium*, 32:3 (2003): 441–456
16. But also notes that, so far, the cyber issue has *not* been securitized. Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*, (Abingdon: Routledge, 2008)
17. Ralf Bendrath, "The American Cyber-Angst and the Real World – Any Link?" In *Bombs and Bandwidth*, ed. Latham; also see, Bendrath, "The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructure Protection," *Information & Security*, 7 (2001): 80–103

18. Robert M. Lee and Thomas Rid, "OMG CYBER! Thirteen Reasons why Hype Makes for Bad Policy," *The RUSI Journal*, 159:5 (2014): 4–12

19. Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security*, 27:5 (2012): 781–799

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

21. One participant observed that a lot of low-hanging fruit remains when it comes to data gathering and analysis. There is still much more to be done in terms of coding these events.

22. President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," (13 October 1997), retrieved from: www.fas.org/sgp/library/pccip.pdf

23. Warner, "Cybersecurity: A Pre-history"

24. It was noted that hybrid warfare, critical infrastructure attacks, and surveillance characterized this regional perspective.

25. Sue Eckert, "Protecting Critical Infrastructure: The Role of the Private Sector," University of Pittsburg, 2006, available at: www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf; Kenneth Neil Cukier, Viktor Mayer-Schoenberger, and Lewis M. Branscomb, "Ensuring (and Insuring?) Critical Information Infrastructure Protection," Working Paper, John F. Kennedy School of Government, Harvard University, 11 October 2005

26. Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks." In H. Rõigas, R. Jakschis, L. Lindström, and T. Minárik (eds.), *Defending the Core*, 9th International Conference on Cyber Conflict, (Tallinn: NATO CCD COE Publications, 2017). The workshop participants did not discuss in any detail the nature of these relationships, whether that interpersonal, agency, or operational.

27. Milton F. Mueller, *Network and States: The Global Politics of Internet Governance*, (Cambridge: The MIT Press, 2010), p. 1

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.