COLUMBIA | SIPA
School of International and Public Affairs

THE CYBER CONFLICT STATE OF THE FIELD WORKSHOP

www.sipa.columbia.edu

CCSA
Cyber Conflict Studies Association

CYBER CONFLICT STATE OF THE FIELD WORKSHOP REPORT

Co-editor: Karl Grindal

Co-editor: Jason Healey

Copyeditor: Emily Walz

ISBN-10: 0-9893274-5-0

ISBN-13: 978-0-9893274-5-9

The School of International and Public Affairs (SIPA) is the world's most global public policy school with a focus on issue realms such as global finance and economics, public health, climate change, energy, development and sustainability-all of which increasingly occupy a transnational space and implicate a global commons, global public goods, and challenges of global collective action. The School's mission, which has evolved over the years, stays true to this history: "SIPA serves the global public interest by educating students to serve and to lead and by producing and sharing new knowledge on the critical public policy challenges facing the global community."

The Cyber Conflict Studies Association (CCSA) is a 501(c)3 nonprofit organization dedicated to promoting and leading a diversified research agenda in the field of cyber conflict. CCSA's vision is to be the premier thought leader in the field by fostering dialogue, leading research, and developing academic programs focused on the implications of cyber conflict.

MODERATOR BIOS

MODERATOR BIOS

Jason Healey is a senior research scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict, competition, and cooperation. Prior to this, he was the founding director of the Cyber Statecraft Initiative of the Atlantic Council where he remains a senior fellow. He is the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012* and co-authored the *Cyber Security Policy Guidebook* published by Wiley. Jason is also a member of the Defense Science Board Task Force on Cyber Deterrence and president of the Cyber Conflict Studies Association. He has been a lecturer in cyber policy at Georgetown University and a lecturer in cyber national security studies at the Johns Hopkins School of Advanced International Studies. Starting his career in the United States Air Force, Jason earned two Meritorious Service Medals for his early work in cyber operations at Headquarters Air Force at the Pentagon and as a plankholder (founding member) of the Joint Task Force – Computer Network Defense, the world's first joint cyber warfighting unit. He has degrees from the United States Air Force Academy (political science), Johns Hopkins University (liberal arts) and James Madison University (information security).

Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and a research fellow at the Hoover Institution, both at Stanford University. His research interests relate broadly to the policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in and knowledgeable about the use of offensive operations in cyberspace, especially as instruments of national policy. In addition to his positions at Stanford University, he is chief scientist, emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology; and adjunct senior research scholar and senior fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Dr. James Mulvenon is vice president of Defense Group, Inc.'s Intelligence Division and director of DGI's Center for Intelligence Research and Analysis. Dr. Mulvenon's latest co-authored book, *Chinese Industrial Espionage* (London: Routledge, 2013), is the first full account of the complete range of China's efforts to illicitly acquire foreign technology. Among his professional affiliations, Dr. Mulvenon is a founding member and current chairman of the board of the Cyber Conflict Studies Association, was a term member of the Council on Foreign Relations between 1999 and 2004, and is presently a member of the National Committee for US-China Relations. He received his PhD in political science from the University of California, Los Angeles, in 1998.

MODERATOR BIOS

Neal Pollard is a director at PricewaterhouseCoopers, where he leads cybersecurity assessments and investigations into cybercrime, economic espionage, and insider threats globally for commercial clients. He is also a nonresident senior fellow at the Cyber Statecraft Initiative at the Atlantic Council's Brent Scowcroft Center on International Security. Previously, he served as a senior officer in the US intelligence community, and prior to government service he was vice president at Hicks & Associates and general counsel and board director at the Terrorism Research Center, a corporation he co-founded in 1996. Mr. Pollard is also an adjunct professor at Georgetown University, and is admitted to the Virginia Bar.

Harvey Rishikof is a senior counsel in Crowell & Moring's Privacy & Cybersecurity and Governments Contracts groups in Washington, DC. He specializes in national security, civil and military courts, terrorism, international law, civil liberties, and constitutional law. Prior to joining the firm, Mr. Rishikof was the dean of faculty at the National War College and former chair of the Department of National Strategy; legal counsel to the deputy director of the FBI; federal law clerk to Leonard I. Garth (Third Circuit); and AA to the chief justice of the United States. He also previously served as dean of Roger Williams University School of Law. Throughout his career, Mr. Rishikof has served on numerous committees and held multiple positions in government focusing on cybersecurity investigations. Most recently, he was the senior policy advisor to the National Counterintelligence Executive (NCIX), the agency responsible for counterintelligence and insider threat management across the federal government. He is a graduate of McGill University and earned an MA from Brandeis University, an MA from the National War College, and a JD from New York Law School.

Dr. Adam Segal is the Maurice R. Greenberg Senior Fellow for China Studies at the Council on Foreign Relations. He is the author of two books on Asia and technology, and his writing has appeared in publications such as the *Financial Times*, the *Washington Post*, the *Los Angeles Times*, *Foreign Affairs*, the *Wall Street Journal Asia*, and the *International Herald Tribune*. He has appeared as a commentator on several networks including Bloomberg, CNN, NBC, NPR, and the BBC. He is also a research associate of the National Asia Research Program. Before working at CFR, Dr. Segal was an arms control analyst for the China Project at the Union of Concerned Scientists. He has been a visiting scholar at the Massachusetts Institute of Technology's Center for International Studies, the Shanghai Academy of Social Sciences, and Tsinghua University in Beijing, and has taught at Vassar College and Columbia University. Dr. Segal has a PhD and a BA in government from Cornell University, and a MA in international relations from the Fletcher School of Law and Diplomacy at Tufts University.

RAPPORTEUR BIOS

RAPPORTEUR BIOS

Erica D. Borghard is an assistant professor in the Department of Social Sciences and executive director of the Grand Strategy Program at the United States Military Academy at West Point. Dr. Borghard received her PhD in political science from Columbia University. Her dissertation, "Friends with Benefits? Power and Influence in Proxy Warfare," explores the dynamics of proxy alliances and proxy warfare, focusing on the mechanisms and complications associated with state control of and influence over nonstate proxies. Her research has appeared in a variety of academic and policy journals, including the *American Political Science Review*, *Survival: Global Politics and Strategy*, and *Parameters*. Dr. Borghard has also published pieces for the Cato Institute, the *National Interest*, CNN.com, and the *Washington Post*.

Justin K. Canfil is a PhD candidate in the Department of Political Science at Columbia University with a minor specialization from Columbia Law. His research focuses on the legal and international security implications of technological diffusion, including cyber. Prior to coming to Columbia, Justin worked as an international affairs and political professional, including a public policy fellowship in the US Congress for a member of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. From 2012-2013, he managed Track II public diplomatic programs on behalf of the US Department of State at the Council on World Affairs in Cleveland. A *summa cum laude* graduate of Ohio State University, he was also a visiting student at the University of Oxford (law) in 2010.

Douglas Cantwell is a lieutenant (junior grade) in the Judge Advocate General's Corps, US Navy. He is currently stationed at the Region Legal Services Office (RLSO) Mid-Atlantic. He previously served as the Detlev F. Vagts international law fellow at the American Society of International Law and has worked for the Geneva Centre for the Democratic Control of Armed Forces and as a research assistant for the Columbia Human Rights Institute. He received his JD from Columbia Law School where he served as head solicitations editor of the *Columbia Journal of Transnational Law* and was a member of the International Fellows Program at Columbia's School of International and Public Affairs. He received an MA from the Graduate Institute of International and Development Studies in Geneva, Switzerland and a BA from Stanford University.

RAPPORTEUR BIOS

Karl Grindal is an Atlanta-based policy analyst and information security researcher. Karl serves as the executive director of the Cyber Conflict Studies Association and is a fellow with X-Lab. He is studying as a PhD student at the Georgia Institute of Technology's School of Public Policy. Before starting at Georgia Tech, Mr. Grindal collaborated with Jason Healey as the associate editor to the book *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Previously, he provided strategic, policy, and research services as director of research for Intelligent Cyber Research, and as a senior analyst at Delta Risk LLC. Mr. Grindal completed a Master's of Public Policy at Georgetown University in 2011.

Shawn W. Lonergan CISSP is an active-duty major in the United States Army and a PhD candidate in the Department of Political Science at Columbia University. Following the completion of a fifteen-month deployment to Iraq in 2008, he was recruited to help the US Army stand up its first provisional cyber battalion where he commanded two expeditionary cyber operations companies. Major Lonergan holds two master's degrees from Columbia and is a graduate of the United States Military Academy at West Point, where he is an assistant professor in the Academy's distinguished Department of Social Sciences and a research scientist in the Army Cyber Institute. Among his other awards, he won the 2013 Atlantic Council's Cyber 9/12 national collegiate competition.

Ryan C. Maness is a visiting fellow of security and resilience studies in the Department of Political Science at Northeastern University. Dr. Maness has published peer-reviewed articles in the *Journal of Peace Research*, *Armed Forces and Society*, and the *Journal of Slavic Military Studies*, as well as in *Foreign Affairs*. He has recently completed two books, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015) and *Russia's Coercive Diplomacy: Cyber, Energy and Maritime Power* (Palgrave Macmillan, 2015). Dr. Maness obtained his PhD degree in political science from University of Illinois at Chicago. •

ACRONYMS

ACRONYMS

- **ABI** - Activity Based Intelligence
- **APTs** - Advanced Persistent Threats
- **CCSA** - Cyber Conflict Studies Association
- **CERTs** - Computer Emergency Response Teams
- **CIGI** - Centre for International Governance Innovation
- **CTBT** - Comprehensive Nuclear-Test-Ban Treaty
- **DDoS** - Distributed Denial of Service
- **DOJ** - Department of Justice
- **DPH** - Direct Participation in Hostilities
- **ETS** - Europe Treaty Series
- **EU** - European Union
- **FBI** - Federal Bureau of Investigation
- **GGE** - Group of Governmental Experts, UN
- **ICANN** - Internet Corporation for Assigned Names and Numbers
- **ICB** - International Crisis Behavior
- **ICC** - International Criminal Court
- **ICJ** - International Court of Justice
- **ICRC** - International Committee of the Red Cross
- **IHL** - International Humanitarian Law
- **INSA** - Intelligence and National Security Alliance
- **IOCs** - Indicators of Compromise
- **IR** - International Relations
- **IT** - Information Technology
- **IW-D** - Information Warfare-Defense
- **JDAMs** - Joint Direct Attack Munitions
- **NATO** - North Atlantic Treaty Organization
- **OCO** - Offensive Cyber Operations
- **OPM** - Office of Personnel Management
- **PLA** - People's Liberation Army
- **POTUS** - President of the United States
- **SCADA** - Supervisory Control and Data Acquisition
- **SCO** - Shanghai Cooperation Organization
- **SIPA** - School of International and Public Affairs
- **TTPs** - Tactics, Techniques, and Procedures
- **UN** - United Nations
- **VPN** - Virtual Private Networks

STATE OF THE FIELD OF CYBER CONFLICT STUDIES: PREFACE

Introduction

In most other fields, there is a frontier of research that explores the boundaries of the possible, but there is also a core body of knowledge shared by the community. In the cyber realm, not only is the research frontier moving faster than in other fields, but it is far more difficult for the community of researchers to simply identify what has already been done. Compared to the rise of air and nuclear power, research into cyber has yet to identify "settled truths." Even though many of the foundational texts are decades old, they are often ignored as more new researchers join a field where so much seems fresh. As the field coalesces, cyber researchers must build on each other's work to create the models, methodologies, and case studies that are desperately needed.

Perhaps the best example of this phenomenon is when new researchers explore questions like, "is a cyberattack an act of war?" With the publication of the *Tallinn Manual* in 2013, this ceased to be a useful research question, compared to examining how the manual categorizes cyberattacks and whether it does so effectively. Likewise, the topic of cyber deterrence or active defense has brought in a flood of researchers with excellent ideas. Unfortunately, some of these inspired new hypotheses were previously introduced several years ago, with some being reinforced over the years and others debunked.

Recognizing the need for an established common ground, the School of International and Public Affairs (SIPA) at Columbia University and the Cyber Conflict Studies Association (CCSA) convened a much-needed workshop on the "State of the Field of Cybersecurity Studies" on June 16th and 17th, 2016 to highlight the current state of knowledge in this burgeoning national security topic. The workshop provided a venue in which to discuss cyber conflict as a field of research, come to agreement on principle research topic areas, review the main questions within each of those topics, create a shared understanding of existing research on those questions, and identify canonical works. Conference organizers identified six major subfields beforehand: international relations, strategic dynamics, tactical operations, history of cyber conflict, intelligence and adversaries, and legal issues.

By bridging these disciplines and sectors, it is possible to establish the building blocks for a new generation of research questions. Through this working conference, we build on the now decade-old work by Dr. James Mulvenon, "Toward a Cyber Conflict Studies Research Agenda," by identifying new questions and methods of discovery for the next decade.

Conference Aims and Structure

Conducted under Chatham House rules, a small group of scholars and practitioners came together to discuss three broad questions:

- Existing Research: What main research questions have dominated scholarly thinking on cyber conflict, around which there is a baseline of consensus?
- Gaps: What notable gaps in the literature would benefit from exploration in future research agendas?
- Canonical Works: What works might be considered "canon"?

Using these questions to frame the discussion, participants aimed to: identify a common body of knowledge with which scholars and practitioners may be expected to be familiar; acknowledge progress and prevent duplication in future research; and shine a spotlight where more rigorous research could expand the frontiers of the field.

INTERNATIONAL RELATIONS / POLITICAL SCIENCE DISCUSSION

Columbia University	**Rapporteur: Ryan C. Maness** **Moderator: Adam Segal**
June 16, 2016	

Introduction

A select group of scholars, policy analysts, and practitioners came together to discuss which topics in international relations (IR) have established consensus among scholars, what may be considered the canonical works of cyber in IR, what research questions are being asked, and what gaps exist in the IR subfield.

The discussion was organized around eight subtopics of cyber conflict and security in the IR field. These subtopics are not mutually exclusive and overlap. The subtopics were:

- How does cyber fit into IR?
- Deterrence and Restraint
- Cyber Power and Influence
- The effects of Cyber on the Structure of the International System
- Cyber Foreign Policy and Doctrine
- The Relationship between State and Nonstate Actors
- Norms and Norm Diffusion
- Cyber Arms Control Institutions and Regimes

The discussion progressed in this order; however, before the main discussion began some participants raised concerns with these subtopics.

Opening Concerns with the IR Categories

Prior to the discussion, there was a somewhat contested debate between the practitioners/policy analysts and academics about the relevance of IR to cyber conflict and security. Practitioners questioned the relevance of IR and its focus on state actors, given the role of nonstate actors in cyberspace. Once nonstate actors are placed at the center of cyber work, practitioners argued, it would be difficult, if not impossible, to apply ideas prominent in IR theory such as deterrence and norms. The academics responded that IR has a rich collection of literature on the behavior of nonstate actors developed through studies of terrorism, intrastate conflict, organized crime, and piracy. Theories and concepts from these studies can explain the motives and actions of various nonstate actors in the cyber realm.

There was further debate about the distinction between cyber and information operations. While in Russia, China, and other states, the use of social media and other forms of influence are considered part of cyber operations, Western analysts and practitioners have traditionally kept the two separate. The participants in the June discussion, however, thought this distinction no longer made sense, and so several studies pertaining to information warfare, particularly the Jaitner and Mattson (2015) study are included in the agreed-upon list of canonical works.

Other issues revolved around category distinctions. Some felt that the norms category was too broad and that there should be a distinction between domestic and international norms. The discussion of international law is described in the "Cyber Arms Control Institutions and Regimes" sub-topic below (and remains one of the larger topics of study). Because bureaucratic politics and foreign policy studies use decisionmaking as their level of analysis, they were merged.

In addition, there was a discussion of whether the full range of IR theories, such as neorealism, neoliberalism, constructivism and the Copenhagen School (securitization theory) were being utilized to explain international cyber conflict, interactions, and governance. Although the main IR theories have all touched on cyber—realism with deterrence and liberalism with cyber institutions and international law applications—constructivist approaches (specifically the Copenhagen school) have been used most often for theorizing about cyber. This raises the question: Why are realists and liberals shying away from cyber theorizing for the most part? What role can critical theory play in theorizing cyber?

Discussion then ensued and was structured as follows:

Topic:	**Question:**	**Gaps:**
How does cyber fit into IR?	Definitional issues. Is cyber a global commons? Exploring the hype: How revolutionary is cyber?	Declining utility? Unexplored areas of IR?

A major question of this sub-topic was: "Have we reached the point of declining utility for articles asking whether or how cyber fits into IR theory?" The works discussed in this particular subtopic included Arquilla and Ronfeldt's (1993) early article on the future of the Internet as a domain conflict; Clarke and Knake's (2010) book about worst-case scenarios in the cyber realm; theoretical works by Kello (2013), Choucri (2012), Rid (2013), Lawson (2013), and Junio (2013); and a theoretical and conceptual debate between Lindsay and Kello (2014). With these works in mind, several questions were asked:

1. **How does cyber affect diplomacy and the hype involved?**

    a. What do we mean by cyber? Does this include the manipulation of code only or should we include information warfare, electronic warfare, and artificial intelligence in the cyber definition as well?

b. Some parts of the cyber realm are not part of a global commons, as we have air-gapped systems such as military networks, VPNs, and other tools that make many parts of cyberspace exclusive and not universally shared.

c. Should there be a more pragmatic outlook on cyber? Doctrinal outlooks are usually products of government and military thinking, and academia can play a crucial role in constructing empirically based non-doctrinal policy recommendations. Therefore, non-doctrinal outlooks are not only necessary, but should be a key focus of cyber academics in the IR subfield.

It was also the opinion of the discussants that this workshop should produce a universally agreed-upon definitional list, much like the ones produced by Fred Kaplan or New America.

2. Is the use of the word "common" or "domain" applicable and does it fit for cyber conflict and security studies? What about the cyber environment?

We need a clear conceptualization of this for cyberspace. How do these differing conceptualizations (domain, common, environment) impact how we look at cyber through the IR lens? Participants decided that the state of field is indeterminate unless this is cleared up.

3. Structure is useful to developing the research of cyber conflict, especially as it relates to IR. What is the nature of the relationship between the organized state and the cyber domain?

Cyber borders: Russia and China and sovereignty. How do states assert control of the domain that challenges territoriality and sovereignty? China, Russia, and other countries insist on the right to exert sovereignty; Western countries stress Internet as a global platform, the free flow of information, and human rights. Is this a point of contention between states that will make cyber conflict more likely? Given this wide political and ideological divide, what common ground can all states find so that agreed upon behaviors and developing norms in cyberspace can begin to develop and take hold?

On a separate but related note, Charles Tilly makes the point that war makes the state and the state makes war. Is use of the term war even a good idea moving the field forward? War in the IR field means something specific and denotes death and casualties, so does the term "war" even have a place in cyber?

Path dependency may be an issue for cyber in the IR subfield. For the United States and much of the West, cyber is thought of in military terms, and therefore the Internet and digital puts us in to the military domain. We should listen to Arquilla and Ronfeldt's early piece and differentiate cyber in military and non-military terms and push forth these separate narratives. China and Russia see cyber through different lenses than the West as well, including control and manipulation of content as well as disruptive attacks. This also must be studied, accepted, and understood to develop the state of the field further.

Topic:	**Question:**	**Gaps:**
Deterrence and restraint	Do the various cyber capabilities of international actors provide deterrent effect in cyberspace? How do you deter cyberattacks and signal intentions?	Lack of new, innovative theories that show how states constrain themselves from cyber action through various interactions, limited number of cases (deterrence failures), continuing definitional issues.

This forum discussed how deterrence theory has been saturating the cyber conflict and security studies field and finds that perhaps we need to move away from this theory and type of thinking. New, innovative, and explanatory theories unique to the cyber environment, actors' behavior and decisionmaking processes, and twenty-first-century strategy need to be developed and backed up with empirical evidence to advance this field. Relying on deterrence strategies for explanation only keeps the state of the field static. Works surveyed on deterrence include Nye (2011), Goodman (2010), Kugler (2009), Libicki (2009), Cooper (2012), and the National Research Council (2010). Valeriano and Maness's (2015, 2016) theory of cyber restraint and Gartzke and Lindsay's (2015) theoretical piece were then offered as alternatives to cyber deterrence as the path forward and will hopefully lay the ground for new theories of cyber conflict. Several questions were raised:

1. Is the nuclear analogy even good?

Not only is the nuclear analogy not good, the case can be made against conventional deterrence thinking as well. If deterrence is about communicating threats by demonstrating or making capabilities known so that one's enemy does not act, then cyber as a deceptive tool in and of itself cannot deter. Attribution can be denied, and states and nonstate actors use cyber with the intention of either not being detected or with the advantageous tactic of plausible deniability.

2. What about psychological studies and cyber?

This is definitely something that needs to be studied by IR and non-IR scholars alike. One particularly useful study that psychology could contribute to cyber conflict and security studies would be psychological profiling of hackers of all hats (black, white, grey).

3. Strategic dynamics of interactions: what actually happens regarding behavior?

Empirical studies are needed for these types of interactions. The International Crisis Behavior (ICB) canonical works in IR can be used as a guide for these types of studies.

4. Maybe deterrence does work but we don't know about it?

Then it would not be deterrence, as deterrence is about clear communication to adversaries. So, we need new ways of theorizing about strategic interactions between entities in the cyber environment. Existing bodies of work in IR, such as the issue-based approach and the study of nonstate actors, are well suited to these tasks, as discussed in this appraisal of the state of the field.

5. Do cyber capabilities provide deterrent effects?

Lindsay and Gartzke have begun looking at cross-domain deterrence with cyber and conventional weapons, yet these studies as yet lack empirical grounding, and remain theoretical.

6. What about defense in the cyber environment? Is it undervalued because of the offense-dominant perception of the cyber environment thus far in cyber conflict studies?

What about risk management? Is it understudied because of cyber's military strategic focus? What can private sector incentivization strategies, such as risk analysis by insurance companies, contribute to cyber conflict and security studies? What can the insurance industry contribute to these risk management studies of cybersecurity and therefore defensive postures in the cyber environment?

What about automated defense and would that contribute to cyber's fit with deterrence? Is automation a good idea? Would states want to make known their

automated defensive structures? This is where deterrence foundations would remain on unstable ground.

Can deterrence work with providing a framework with escalatory risk? In other words, can we raise the costs of potential hackers and deter them in the cyber environment this way? There are few to no empirical studies that have shown this to be true as of yet, but it is an avenue worth exploring in the IR field.

7. **Again, how do nonstate actors fit into this?**

The theory of cyber restraint (Valeriano and Maness 2015) can be applied to nonstate behavior. Again, deterrence may be a dead end for cyber conflict studies due to the deceptive nature of many offensive cyber tools and methods. Deterrence works because of fear of the known; restraint is better because it takes fear of the unknown (cyber deception) into account. Gartzke and Lindsay's (2015) "Weaving Tangled Webs" is definitely canonical in this regard.

Topic:	**Question:**	**Gaps:**
Power and Influence	What is cyber power and how do we measure it? What does net assessment mean for cyberspace? What is influence in cyberspace?	Empirical studies on cyber power, an examination of cyber through the lens of soft power.

This discussion focused on a topic all too familiar to those in the field of IR: power. Should we look at cyber power as a form of hard power? Or can cyber be better understood through a soft power lens? How would we measure cyber power both theoretically and empirically? These questions were discussed through cyber power literature including works by Kramer, Starr, and Wentz (2009), Sheldon (2012), Nye (2010), Segal (2016), Betz and Stevens (2012), Healey (2013), Rid and McBurney (2012), Lindsay (2013), Rattray (2001), and Libicki (2007). Several overarching questions were asked and discussed in this forum:

1. **Measuring cyber power: How do we do it? What do we include? Who is the most powerful? The will to use power confers credibility. If existing measures usually count tangible things, how can this be adjusted for cyber, especially since many aspects of cyber power are confidential, deceptive, or intangible?**

Concrete analysis of power for cyber: Suggestions for measuring tangible cyber power empirically included spending (military and non-military private sector), IT education, IT infrastructure, offense, defense, and an analysis of vulnerabilities (where the more plugged-in may be the more vulnerable).

2. **Would measuring cyber vulnerabilities help measure power? In other words, would the least vulnerable states be the most willing to use cyber? Would this give the advantage to non-democratic states?**

3. **Cross-domain and additive power of cyber: Does a state's use of cyber combine with conventional uses of power to make it more powerful? How would we know? How does having hard power in other domains affect cyber power?**

4. **Country-specific: Who has the power? On defense, bad cyber hygiene can make a state weak and the nonstate actor more powerful. so should we conceptualize offense differently? How is cyber power diffused to nonstate actors?**

   a. Does the diffuse structure of the US network make it less powerful than the centralized control of Russian and Chinese networks?

   b. Does Russia's mobilization of nonstate actors on its behalf give it more power? Is there a power difference between democracies and non-democracies as a result? Do authoritarian states have an edge?

5. **The United States is an offense cyber power, but not known for defense. Why?**

Topic:	**Question:**	**Gaps:**
The Effects of Cyber on the Structure of International Relations: Attribution/ Offense versus Defense/ Strategic Instability	Is cyber offense dominant? Is too little attention paid to defensive capabilities?	More in-depth analyses of the defensive side, new thought on offense-defense balance dynamics based on unique characteristics of the cyber domain, and methods for evaluating technological change and innovation

As many of the questions regarding this subtopic were covered in previous subtopic discussions, not much time was spent on offense/defense dominance. However, three questions came out of this subtopic and are worth noting due to their importance to forwarding the state of the field in IR. Works in this subtopic of IR include Liff (2012), Rid and Buchanan (2014), Valeriano and Maness (2014), Gartzke (2013), Andres (2012), Saltzman (2013), Peterson (2013), and Fielder (2013).

1. **Cyber aids strong, not weak states: States with more power and resources have more rapidly developed cyber capabilities.**

   The United States, Russia, and China are the preeminent cyber powers. This challenges the idea that cyber power is diffuse. However, Israel may be the exception to this rule, as it definitely punches above its weight in the cyber realm. Does this bode well for other less-powerful states and even nonstate actors?

2. **Attribution is not just a technical act.**

   IR can place attribution into a larger context and help assist with attribution to actors based on established political and strategic considerations. It can also seek to address questions like: How complicit is a state in a cyber attack committed by a nonstate actor within its territory? Should states assign varying levels of blame? Cyber attribution does not need to be proven beyond a reasonable doubt; Healey's attribution scale as well as Rid and Buchanan's (2014) work can help start a new attribution debate beyond technical forensics.

3. **Is there value for states in declaring a policy on attribution and blame?**

   Could this be the path forward to make deterrence work in the cyber environment? More empirical studies in this regard are needed and this is a topic where IR can contribute to further the state of the field.

Topic:	**Question:**	**Gaps:**
Cyber Foreign Policy and Doctrine	What is the foreign policy impact of cyber operations and what guides the foreign policy doctrines of specific actors? How do certain conditions and state institution dynamics explain the cybersecurity polices of states?	There are few in-depth studies of decisionmakers as they make cyber policy, studies of nations beyond Russia, the United States, China, Israel, and the UK.

Many diverse questions were raised in this discussion, showing that this subtopic may be where IR can most contribute to furthering cyber conflict and security studies. Works highlighted in this discussion include: Maness and Valeriano (2016); Geers (2015); Gvosdev (2012); Jaitner and Mattson (2015); Inkster (2013, 2016); Lindsay (2015); Lindsay, Cheung, and Reveron (2015); Segal (2013); Gompert and Libicki (2014); Dunn-Cavelty (2008); Reveron (2012); Guitton (2013); Axelrod and Iliev (2014); Kaplan (2015); Junio (2013); Yannakogeorgos (2012); and Yannakogeorgos and Lowther (2013). Many unanswered questions remain. Among them:

1. **Has the United States militarized the concept of cyber, and if so, how does this guide IR scholarship? Should we move to focus on multi-stakeholder frameworks where nonstate and non-military actors play a bigger role?**

2. **It is glaringly apparent that the field needs larger comparative studies on how countries think about cyber and implement policy. Should these be descriptive or normative?**

3. **Do we see norms changing the policies of states? Should future IR studies be descriptive first and then turn to normative and prescriptive studies?**

4. **Do we need a new policy/prescriptive category, and if so, how should IR proceed in this matter? Can IR take the lead in empirically based policy prescriptive studies?**

5. **There is an oversaturation of books and papers about cyber decisionmaking and policy in the United States, Russia, and China. What about North Korea, Iran, the EU, Japan, and other nations? We need more comparative case studies of countries and their cyber doctrines.**

6. **Rational choice and game theory can be applied to cyber conflict and security studies and this should be a clear path forward for the field.**

7. **How are the activities of foreign state actors assessed? How do perception and misperception and the security dilemma work in cyber conflict decisionmaking? Jervis's work could be applied here**

8. **More in-depth nonstate group studies are needed, not just at levels below the state, but at levels above as well (supranational). As discussed above, this is an area where IR can take the lead, as it already has a basis of literature to build upon.**

9. **What is the functionality of international organizations in cyber? What can we learn from NATO, ICANN, SCO, the EU, and others?**

Topic:	**Question:**	**Gaps:**
The Relationship between State and Nonstate Actors	How does the diffusion of power in the cyber realm change the international landscape?	Empirical assessments of nonstate actors' capabilities and the threats they pose.

Given the overarching concerns about the general utility of IR's state-based approach with the prominence of nonstate actors in cyber conflict and security studies, this subtopic filtered into discussions on many of the other subtopics. Nonstate actors are being considered and studied in IR, although many areas of the field have not yet adequately considered their impact. Two important studies on nonstate cyber actors (Weinmann 2015, Benson 2014) were included in this short discussion, out of which came two questions:

1. **How many nonstate actors are aligned or non-aligned with states? Good idea for study; Valeriano and Maness are beginning to collect data on nonstate incidents.**

2. Should we include corporations such as Microsoft and Google as nonstate actors?

Maybe not. In the field of IR, nonstate actors usually have a combative and malicious intent. Legitimate actors such as Microsoft would be considered NGOs; therefore, we should keep in line with IR definitional protocol.

Topic:	Question:	Gaps:
Norms and Norm Diffusion	How do we promote norms in cyberspace? Do we need new specific norms for the cyber realm or do existing norms apply? How are state and nonstate actors engaged in norm entrepreneurship? What comparisons can be drawn to other to other examples, such as land mines?	Liberal theories of normative behavior, more non-Western points of view on normative arguments

The primary focus of discussion in this subtopic was whether existing international norms can apply to the cyber environment, or if new norms need to be developed to govern cyberspace in the international arena. This is a subfield where the liberal theory of IR can play a key role in propelling the field forward. Democracies, markets, and human rights promotion can encourage the international discourse that has allowed for a relatively prosperous world order under US leadership since the end of the Cold War. Can liberalism provide new ideas on the path forward for a safe and prosperous international cyber environment? The Copenhagen School has already taken the lead regarding norms and norm diffusion; liberal theories could serve as a diversifying addition to this subtopic. Works that formed the basis of this discussion include those from Mazanec (2015), Nissenbaum (2005), Hansen and Nissenbaum (2009), Dunn-Cavelty (2015), Maurer (2011), and Grigsby (2015). The discussants explored several questions:

1. Was 2015 a breakout year for international cyber norms?

Organizations such as the G7, G20, Microsoft, and the UNGGE have all produced detailed, agreed-upon modes of expected behavior for state governments in the cyber environment. Was the OPM hack the catalyst? Has US leadership helped in this regard? What other factors could have contributed to make this the year of cyber norms?

2. Are norms effective?

It could be argued that they are in terms of reinforcing already-constrained behavior from states; however, state-sponsored espionage is largely excluded from international norms. Should this change for the cyber realm?

3. Are we able to identify norms in cyberspace?

At least in theory, we need more empirical studies confirming restrained behavior from actors to show the existence of norms.

4. If we can identify norms in cyber, what evidence do we have that they are working?

There are norms regarding the overt use of cyber weaponry in place: SCADA systems remain largely untouched aside from a few high-profile incidents, so for the most part, the answer is yes. The problem remains with the use of cyber for information manipulation, theft, and nonstate cybercrime: how do we make norms for these, and how can IR contribute?

5. Are norms effective?

It could be argued that they are in terms of reinforcing already-constrained behavior from states; however, state-sponsored espionage is largely excluded from international norms. Should this change for the cyber realm?

6. Realist theory would suggest that a lack of norms promotes aggression.

Does a lack of aggression mean there are norms in place that are working? Should we push for norms or legal frameworks in the international arena? Do we need the latter? Perhaps for the international level we should push for norms over law in cyber, as the burden of proof in cyber makes enforcement trickier.

7. Are there operational-level norms with expiration dates? Good exploratory question for future research.

8. Are there no norms for espionage and is this okay for cyber?

The G20 is against commercial espionage, but allows for political and military spying. Recent reports say that China has reduced its intellectual property espionage since the Xi-Obama meeting in September 2015.

9. Why has more progress seemingly been made in cyber norms than in other areas of the cyber IR field?

Topic:	**Question:**	**Gaps:**
Cyber Arms Control Institutions and Regimes	How do we regulate cyber weapons proliferation due to the stark differences in tangible assessment capabilities that are present in the other domains (i.e., conventional weapons are more visible and countable?	Original ideas on institutions, treaties, and conventions for cyber weapon proliferation; conditions for cooperation.

This discussion also revolved around whether existing frameworks regarding institutions and regimes can be applied to the cyber environment. This is another subtopic where neoliberal institutionalism could provide a breakthrough for future research. What about biological and chemical weapons treaties? What about the Just War tradition? Can we apply these to cyber arms control and cyber conflict initiation and prevention? Studies surveyed for this forum include works from Dipert (2010), Schmitt (2013), Knake (2014), Lin (2012), Valeriano and Maness (2015), and Geers (2010). Several questions were raised in the discussion:

1. Are biological and chemical weapons comparisons fair?

Comparative studies are useful, but we also need to be original in our thinking due to the unique characteristics of cyber. Comparisons to these types of weapons regimes may not apply to the cyber realm.

2. What is a cyberweapon? How do we define it, and where is the line drawn? Do only states possess cyberweapons? This is a question to which no one seems to have an answer.

3. **How do we define the goal of arms control? This is a good question and needs to be studied further.**

4. **How is the US government using cyberweapons? Are they stockpiled? What does a cyber arms race look like? What do we count and what do we control? How do we enforce treaties and regimes and verify that they are being followed? Does the UN take the lead in this regard?**

5. **Consent, verification, and enforcement are needed to control an arms race, but what specifically needs to be controlled? Should the focus be on procurement or usage? Regarding cyberweapons, what does a cyberwar look like? Do death, injury, and civilian casualties have to be involved?**

The smaller moderated discussion then moved to a larger forum where all academics, practitioners, and policy experts converged and had the opportunity to discuss the applications of IR to cyber.

Plenary discussion

1. What's the big deal about saying which theory is right? Different theories are able to explain different parts of cyber; so let's acknowledge it and move on. It seems that theoretical debates may be stymieing progress in the IR field of cyber conflict and security studies.

2. If we use different theories to get perspective on the problems of cyber, more decisive canonical works can be categorized and the state of the field can get richer.

3. Humans can't command and control cyberwarfare, so should we automate? What are the threats from automation?

4. Cyber is fast in execution but slow in development; a lot of planning and money is behind it.

5. What amount of effort is need for planning and intelligence collection in cyberwarfare, and what utility is achieved from successful operations? These kinds of questions require a lot of behavior patterns, and IR is arguably prepared to tackle this complicated task.

6. States don't play by the same rules as others. This is true, yet IR is equipped to unpack the behavior of nonstate actors as well.

7. Do we need a universal grammar of engagement for cyber? In other words, do we need a vocabulary of escalation? In the United States, we need an agreed-upon state of norms. What about the G20?

8. The Sony hack: can we escalate in cyberspace? Economic sanctions were the choice of retaliation for this event. Was this the correct response and how effective was it? Was the Sony hack that big of a deal or did it show the lack of hygiene on Sony's part due to the fact that North Korea tore it apart? We need to think not just offensively and escalatory, but in defensive and competence terms as well.

9. So we need to create the proper responses for cyber? Would this be scalable? Should it be Just War style (proportional)? Is a cyber response the only proportional response, or are conventional responses acceptable as well?

10. We need a vocabulary about the operational and tactical facets of cyber so that we can be better at constructing these modes of behavior.

11. There is not a cyber commons: is it sovereign and Westphalian? Conceptions of the Internet are different between Russia, China, the United States and even Europe, so no is the multi-stakeholder model folly? This is seen in other domains between the West and Russia/China; can make applications and not jump the gun here regarding treating cyber governance differently. IR can lead the way here.

12. What's different about cyber in terms of escalation? In the cyber domain exclusively? Or cross-domain too? So far not much spillover into other domains, and most cyber responses have not been escalatory; but what about the future?

13. We have norms and laws but still have the capabilities to do real harm. Can we really prevent this? If they aren't being used en masse do we need to try to coerce states into banning them? Won't that promote bad behavior?

14. We've lost the ability to call out certain international behaviors, especially in cyber. That's because we look at attribution in technical and legal lenses. The IR lens could help with attribution by placing it in a political context as well.

15. Ceded attribution to the private cybersecurity companies, and relying on these can be bad. Private security companies have an incentive to sell their products and an anarchic cyber environment can perpetuate this and lead to escalatory responses by states.

16. Are comparative frameworks good applications to cyber normative practices? Capabilities are being produced but not used; is this acceptable and sustainable?

17. How effective are *sus generis* practices? We do see restraint (capabilities do not match actions).

18. Three images (Waltz) of cyber power...individual, state, and system; is this how we can look to empirically measure cyber power?

19. What about two-level games and their applications to studying cyber behavior? We have an Industry of insecure products; and this subsequently leads to all of the problems regarding threat perception and vulnerabilities. There are also a lot of vulnerabilities on the human side, and studies about the lower level game of the domestic constituency can uncover some interesting studies about making all networks more secure.

20. Customary norms can survive the cyber realm. May agreed to this premise but we also can create *sus generis* ones too.

21. Is the premise of a free and open Internet good for security? Do we have a choice?

Conclusion

Is there anything in IR cyber that is settled? Or have we just agreed on what we're looking for? There is no question that IR has not uncovered many of the burning questions that need to be answered about cyber conflict and security. Yet this does not make IR obsolete or ill equipped to uncover these pressing questions. Cyber conflict can be studied using existing IR theories and IR can answer these pressing questions at the systemic, state-level, and nonstate level. There are existing studies in other areas of conflict that IR scholars can turn to for guidance. Yet at the same time, we must treat the cyber environment as a unique environment where strategic and operational considerations may de different than other domains. It is here where IR scholars must be theoretically innovative and empirically grounded for the state of the field to move forward and continue to produce groundbreaking canonical works that can help lead to a safe and prosperous cyberspace. •

Andres, Richard. “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence.” In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012. http://www.jstor.org/stable/j.ctt2tt6rz.

Arquilla, John and David Ronfeldt. “Cyberwar Is Coming!” Comparative Strategy 12, no. 2 (April 1, 1993): 141–65. doi:10.1080/01495939308402915.

Axelrod, R. and R. Iliev. “Timing of Cyber Conflict.” Proceedings of the National Academy of Sciences 111, no. 4 (January 28, 2014): 1298–1303. doi:10.1073/pnas.1322638111.

Benson, David C. “Why the Internet Is Not Increasing Terrorism.” Security Studies 23, no. 2 (April 3, 2014): 293–328. doi:10.1080/09636412.2014.905353.

Betz, David J. and Tim Stevens. Cyberspace and the State: Towards a Strategy for Cyber-Power. 1 edition. London, UK: Routledge, 2012.

Choucri, Nazli. Cyberpolitics in International Relations. Cambridge, Mass.: MIT Press, 2012.

Clarke, Richard A. and Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. Reprint edition. New York: Ecco, 2011.

Cooper, Jeffrey. “A New Framework for Cyber Deterrence.” In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012: 105-120. http://www.jstor.org/stable/j.ctt2tt6rz.

Dipert, Randall R. “The Ethics of Cyberwarfare.” Journal of Military Ethics 9, no. 4 (2010): 384–410.

Dunn Cavelty, Myriam. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge, 2007. http://www.tandfebooks.com/isbn/9780203937419.

———. “The Normalization of Cyber-International Relations.” In Strategic Trends 2015, 81–98. Zurich, Switzerland: Center for Security Studies, 2015. https://www.researchgate.net/publication/274076687_The_Normalization_of_Cyber-International_Relations.

Fielder, James D. “Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion.” Small Wars Journal 9, no. 6 (June 19, 2013). http://smallwarsjournal.com/jrnl/art/bandwidth-cascades-escalation-and-pathogen-models-for-cyber-conflict-diffusion.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” International

Security 38, no. 2 (October 2013): 41–73. doi:10.1162/ISEC_a_00136.

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. doi:10.1080/09636412.2015.1038188.

Geers, Kenneth. Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: CCDCOE, 2015. http://scholar.google.com/scholar?cluster=9137378561972954249&hl=en&oi=scholarr.

———. "Cyber Weapons Convention." Computer Law & Security Review 26, no. 5 (2010): 547–551.

Gompert, David C. and Martin Libicki. "Cyber Warfare and Sino-American Crisis Instability." Survival 56, no. 4 (July 4, 2014): 7–22. doi:10.1080/00396338.2014.941543.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" US Senate Washington, DC Committee on Armed Services 4, no. 3 (Fall 2010). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA528033.

Grigsby, Alex. "The UN GGE on Cybersecurity: What Is the UN's Role?" Council on Foreign Relations - Net Politics, April 15, 2015. http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/.

Guitton, Clement. "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?" European Security 22, no. 1 (March 2013): 21–35. doi:10.1080/09662839.2012.749864.

Gvosdev, Nikolas K. "The Bear Goes Digital: Russia and Its Cyber Capabilities." In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, edited by Derek Reveron. Washington, DC: Georgetown University Press, 2012. http://www.jstor.org/stable/j.ctt2tt6rz.

Hansen, Lene and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." International Studies Quarterly 53, no. 4 (December 2009): 1155–75. doi:10.1111/j.1468-2478.2009.00572.x.

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

Inkster, Nigel. China's Cyber Power. The International Institute for Strategic Studies, 2016.

———. "Chinese Intelligence in the Cyber Age." Survival: Global Politics and Strategy 55, no. 1 (March 2013): 45–66. doi:10.1080/00396338.2013.767405.

Jaitner, Margarita and Peter A. Mattsson. “Russian Information Warfare of 2014.” In Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference on, 39–52. IEEE, 2015. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7158467.

Junio, Timothy. “A Theory of Information Warfare.” University of Pennsylvania dissertation, 2013.

———. “How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate.” Journal of Strategic Studies 36, no. 1 (February 1, 2013): 125–33. doi:10.1080/01402390.2012.739561.

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

Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” International Security 38, no. 2 (October 17, 2013): 7–40.

Knake, Robert K. Internet Governance in an Age of Cyber Insecurity. Council Special Report, no. 56. New York, NY: Council on Foreign Relations, 2010.

Kramer, Franklin, editor. Cyberpower and National Security. 1st edition. Washington, D.C: Potomac Books, 2009.

Kugler, Richard L. “‘Deterrence of Cyber Attacks,’” In Cyberpower and National Security, edited by Franklin Kramer, Stuart H. Starr, and Larry K. Wentz, 1 edition. Washington, D.C: Potomac Books, 2009: 309-42

Lawson, Sean. “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats.” Journal of Information Technology & Politics 10, no. 1 (January 2013): 86–103. doi:10.1080/19331681.2012.759059.

Libicki, Martin C. Conquest in Cyberspace: National Security and Information Warfare. 1 edition. New York, NY: Cambridge University Press, 2007.

———. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND, 2009. http://www.books24x7.com/marc.asp?bookid=54204.

Liff, Adam P. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” Journal of Strategic Studies 35, no. 3 (June 2012): 401–28. doi:10.1080/01402390.2012.663252.

Lin, Herbert S. “Arms Control in Cyberspace: Challenges and Opportunities.” World Politics Review, March 6, 2012.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22, no. 3 (July 1, 2013): 365–404. doi:10.1080/09636412.2013.816122.

———. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security 39, no. 3 (Winter 2014): 7–47.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, editors. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. 1 edition. Oxford University Press, 2015.

Lindsay, Jon R. and Lucas Kello. “Correspondence: A Cyber Disagreement.” International Security 39, no. 2 (October 2014): 181–92. doi:10.1162/ISEC_c_00169.

Maness, Ryan C. and Brandon Valeriano. “The Impact of Cyber Conflict on International Interactions.” Armed Forces & Society 42, no. 2 (April 1, 2016): 301–23. doi:10.1177/0095327X15572997.

Maurer, Tim. “Cyber Norm Emergence at the United Nations—An Analysis of the UN’s Activities Regarding Cyber-Security.” Belfer Center for Science and International Affairs, Harvard Kennedy School, discussion paper, September 2011. http://belfercenter.ksg.harvard.edu/publication/21445/cyber_norm_emergence_at_the_united_nationsan_analysis_of_the_uns_activities_regarding_cybersecurity.html.

National Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing

Strategies and Developing Options for U.S. Policy, (Washington, DC: The National Academies Press, 2010).

Mazanec, Brian M. The Evolution of Cyber War: International Norms for Emerging-Technology Weapons. Lincoln, NE: University of Nebraska Press, 2015.

Nissenbaum, Helen. “Where Computer Security Meets National Security.” Ethics and Information Technology 7, no. 2 (June 2005): 61–73. doi:10.1007/s10676-005-4582-3.

Nye, Joseph S. “Cyber Power.” Essay from the Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html.

———. “Nuclear Lessons for Cyber Security?” Strategic Studies Quarterly 5, no. 4 (Winter 2011): 18–38.

Peterson, Dale. “Offensive Cyber Weapons: Construction, Development, and Employment.” Journal of Strategic Studies 36, no. 1 (February 2013): 120–24. doi:10.1080/01402390.2012.742014.

Rattray, Gregory J. Strategic Warfare in Cyberspace. Cambridge, Mass: MIT Press, 2001.

Reveron, Derek S., editor. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, DC: Georgetown University Press, 2012.

Rid, Thomas. Cyber War Will Not Take Place. London: Hurst & Company, 2013.

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

Rid, Thomas and Peter McBurney. "Cyber-Weapons." The RUSI Journal 157, no. 1 (February 2012): 6–13. doi:10.1080/03071847.2012.664354.

Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance." Contemporary Security Policy 34, no. 1 (April 2013): 40–63. doi:10.1080/13523260.2013.771031.

Schmitt, Michael N., editor. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, Mass.: Cambridge University Press, 2013.

Segal, Adam. "The Code Not Taken: China, the United States, and the Future of Cyber Espionage." Bulletin of the Atomic Scientists 69, no. 5 (November 27, 2015): 38–45. doi:10.1177/0096340213501344.

———. The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. First edition. New York: Public Affairs, 2016.

Sheldon, John B. "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War." In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012L 207-224.

Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution." Journal of Conflict and Security Law 17, no. 2 (July 24, 2012): 229–44. doi:10.1093/jcsl/krs019.

Valeriano, Brandon and Ryan C. Maness. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011." Journal of Peace Research 51, no. 3 (May 1, 2014): 347–60. doi:10.1177/0022343313518940.

SECTION

TACTICAL AND OPERATIONAL DYNAMICS OF CYBER CONFLICT

Columbia University	**Moderator: Herb Lin** **Rapporteur: Shawn Lonergan**
June 16, 2016	

Introduction

Armed conflict occurs at different levels—tactical, operational, and strategic—which are hierarchically organized and mutually supporting. In an ideal Clausewitzian, linear model of warfare, all of these levels are directed toward the attainment of a political objective, which defines the dynamics at each stage. In other words, policy directs the strategy employed to achieve it, strategic dynamics shape the nature of operations, and operations structure tactics. This model stands in contrast to the circular model of warfare, wherein dynamics at lower levels of warfare shape strategic decisions and even policy objectives. This chapter builds on previous examinations of the strategic level of cyberwarfare to assess how to define and conceptualize the tactical and operational levels of cyberwarfare and to examine the state of the field as the academic discipline has approached it.

The strategic level of warfare is said to be the decisive level; it is in this realm that outcomes of victory or defeat are determined. Strategy links a government's overall policy objectives with the dynamics on the battlefield in support of them. It provides the overarching framework and guidance for the direction of warfare. The operational level of warfare is concerned with organizing a state's armed forces for the purposes of carrying out campaigns in a particular theater in support of the overall strategy. Tactical warfare occurs at the level of the battlefield where organized armed forces engage one another in combat.

With the emergence of a new domain of warfare (that is, cyberspace), tactical and operational questions have taken precedence over strategic ones—perhaps due to the unique complexities associated with the latter. What this implies for the international system remains to be seen. However, thus far political actors have been engaging at the operational and tactical levels in something approximating a strategic vacuum. Therefore, in one sense, it is intellectually incomplete to explore the dynamics of the operational and tactical levels of cyberwarfare absent a rigorous review of its strategic dynamics. Nevertheless, the sheer fact that political actors are primarily engaging on operational and tactical levels forces a consideration of questions regarding the employment of cyber force at these levels; the legal and ethical implications of doing so; issues associated with command and control; variations across different types of states; and the merits of creating a Cyber Service.

Employing Cyber Power at the Operational and Tactical Levels

While it widely known that actors are employing cyber capabilities on a regular basis on both the tactical and operational levels of warfare, the details of these engagements are not disseminated to the public or to academics. This complicates efforts to understand the reality of cyber tactics and operations, or to speculate about future trends. Nevertheless, fundamental concepts regarding the nature of cyberwarfare can be distilled from consistent attributes of the technology that existing case studies have revealed.

Cyber operations and tactics are different from conventional ones, in part due to the unique nature and scope of the battlefield. In conventional warfare, the battlefield is clearly defined within the various domains. On land and at sea, the scope of the battlefield is limited by geography: land warfare occurs on a particular piece of territory; naval engagements occur at sea. Air power most closely resembles the cyber domain because the air domain is a conduit to conduct attacks against targets across all domains. In other words, the attacks can be delivered via air against targets on the land, targets at sea, and other airborne targets. The battlefield in cyberspace can be defined as any networked system, which may or may not be connected to the Internet.

The relatively short history of cyberwarfare has demonstrated that certain effects can be achieved at the operational and tactical levels. At the tactical level, attacks are defined by singular engagements. These may include disruptive attacks against critical infrastructure, such as DDoS attacks against financial institutions and private corporations, and is defined by contact with the “enemy.” The tactical dynamics of a singular cyber engagement revolve around how an offensive actor maximizes impact, while the defender minimizes impact and tries to learn from the opponent. At the operational level, destructive attacks against command and control and various communication systems may shift the capability of an opponent. Or effect may be measured based on iterative attacks that yield leverage in the form of knowledge or reduced willingness to fight. Particularly in the realm of electronic warfare, operational level dynamics are used to support conventional military operations including precision targeting, disabling adversary air defenses, and aiding intelligence collection.

Known capabilities provide a reasonable basis for projections about the near-term future of cyber operations and tactics. Capabilities are likely to change based on three different types of developments. First, as the technology associated with cyber power evolves, new types of tactics and operations can become technically feasible. Conversely, this same evolution could present states with new vulnerabilities as they become more reliant on interconnected networks and systems. The overall security

environment will also change, as new organizations, business models, and functions form that shift the capacity of states to respond.

Second, military planners, policymakers, and academics can evolve their thinking on force employment in cyberspace, develop new doctrines and organizational approaches that change how governments use both existing and new capabilities, and integrate them with conventional ones.

This discussion suggests several avenues for further research:

- What effects have cyber operations had on the tactical and operational levels of war, and what effects could they have in the future?
- To what extent does the level of classification that surrounds military cyber operations inhibit their use?
- What are the qualitative and quantitative training benchmarks that actors need to establish for cyber forces to function at a high level?
- What are the barriers to entry for creating an offensive cyber force?
- What kinds of effects can actors deliver in cyberspace absent significant advance preparation?
- What differences exist across states (and/or state types) concerning the doctrinal employment of cyber capabilities in pursuit of tactical and operational objectives?
- Is cyberwarfare offense or defense dominant? How would we measure the offense-defense balance in cyberspace?
- In the tactical and operational space, what is the relationship between state and nonstate actors?
- Is it possible and/or necessary to develop a taxonomy of the effects and instruments used in cyber operations and tactics?

Legal and Ethical Considerations

International law governing armed conflict is traditionally divided into two distinct categories: *jus ad bellum* and *jus in bello*. The former category—the conditions under which entering into an armed conflict is just—is outside of the scope of questions regarding the use of force at the tactical and operational levels once armed conflict has been declared. For this reason, this chapter focuses on the latter category but acknowledges that research that grapples with the legal and ethical implications of offensive cyber operations conducted outside of the scope of declared war and ongoing hostilities is needed, as these represent the bulk of offensive cyber operations observed to date.

The key question at stake is how, and the extent to which, the considerable body of jurisprudence pertaining to armed conflict applies to the cyber domain. Laws of

armed conflict, for instance, specifically delineate who counts as a combatant versus a noncombatant, with implications for targeted strikes; how to conceptualize proportionality of responses in warfare; and the obligations of combatants to take precautions to prevent noncombatant casualties. The unique interconnectedness of civilian and military spheres in the cyber domain further complicates the application of international law.

It is far more difficult to distinguish, for instance, what constitutes a purely military target from a civilian one. For instance, some government networks ride on the backbone of the civilian Internet. Moreover, the human capital resources that a state could marshal in support of cyber operations blur the distinction between combatant and noncombatant. It is not clear how the laws of war apply to non-uniformed individuals conducting offensive cyber operations on behalf of a government. Additionally, there is no agreed-upon metric to gauge a proportionate response to a cyberattack, or measure proportionality in using a cyberattack to respond to a conventional one. Furthermore, there is no agreement among the major players in this domain concerning the applicability of the laws of armed conflict. For example, states such as Russia and China do not agree that international humanitarian law applies to the cyber domain.

Finally, even absent established international law, the international relations literature acknowledges that international norms can also constrain state behavior in the absence of a legal regime. However, in cyberspace, there are no widely accepted norms regarding the use of cyber capabilities.

Perhaps the absence of international laws and norms regarding the use of cyber power in the context of armed conflict stems from the fact that full integration of highly disruptive cyber operations with armed conflict has yet to be demonstrated at scale. However, Russian incursions into Georgia in 2008 and Ukraine in 2014 may provide the closest examples to date. The history of international law suggests that it often takes a new form or nature of conflict to prompt states to establish legal regimes. For instance, it took the American Civil War to prompt the United States to develop the Lieber Code, which influenced the development of international laws of war.

The following research questions stem from the above discussion:

- To what extent is existing international law applicable to the cyber domain?
- What are the conditions under which an international consensus regarding the use of force in cyberwar is likely to emerge?
- Are there informal mechanisms that may arise to shape state behavior in the context of cyberwarfare absent legal regimes and norms?
- The infrastructure in the cyber domain is very much entangled between private and public spheres. How does this impact the laws of war for targeting?
- What is the significance of silence about various offensive cyber operations? Iran didn't complain about Stuxnet in any international forum, for example. Does this make the world legally safer for more stuxnets in the future?

Command and Control Considerations

Militaries have long relied on rigid hierarchies for delegating authority for the use of combat power at the tactical and operational levels. However, in the cyber domain, this delegation has not yet occurred. In the United States, for instance, the president retains all authority on the execution of cyberattacks and some (but not all) espionage operations.

This has important implications for the tactical and operational levels of warfare, because a lack of structurally delegated authority could inhibit the timely use of cyber capabilities. Furthermore, this lack of delegation has implied that offensive cyber operations can only be conducted very deliberately and, for the most part, have been integrated into operations and contingency plans at the national level. In some ways, this is similar to drone warfare, where US Army commanders at the brigade level and below, despite being entrusted with thousands of troops and equipment, do not have organically assigned missile-armed drones.

The history of modern warfare has provided ample evidence in support of the benefits of delegating authority to lower levels of command, because it enables commanders to exploit opportunities and take initiative when opportunities present themselves. Therefore, it is important to explore the extent to which existing command and control structures may hinder or otherwise negatively impact battlefield dynamics in ways that could end up having strategic effects:

- What is the proper level of delegation of authority for the command and control of offensive cyber operations? How might these authorities vary by mission type?
- Do we need a cyber-SIOP or a cyber tasking order?
- Should the authority to employ cyberweapons require the authorization of the President of the United States, as is the case with nuclear weapons, or can this authority be devolved?

Organizational Considerations

How should a state recruit, equip and train its force in cyberspace to effect objectives at the tactical and operational levels of warfare? These organizational questions are difficult not only due to debates about proper authorities, but also because of the limited pool of talent from which governments can draw to populate their cyber forces. To be effective at the operational or tactical level in cyberspace, states need well-trained operators (armed with the right capabilities, against the appropriate vulnerable targets) who have received the authority to conduct the operations. Getting all of the elements right is incredibly difficult. Governments are still struggling to identify how to best organize their cyber forces to achieve desired effects.

Furthermore, there is notable variation across states in terms of how they have approached organizing their cyber forces. Some of this variation could be attributed to regime type. For instance, many authoritarian regimes develop cyber forces to engage adversaries both at home and abroad. These priorities affect how governments approach training and equipping their cyber forces. They may be wary about providing these forces with certain tools and accesses, just as these regimes are averse to giving their militaries capabilities that could be used against them. Similarly, the objectives a state seeks to achieve in cyberspace may also shape its organizational approach, namely, whether it organizes for mass or tailored operations.

Historically, countries have organized around domain-centric warfare. Armies fight on land; navies at sea; the air force in the air. The emergence of a new domain raises the question of whether cyberspace merits its own service. One may argue that it is easier to integrate cyber capabilities into conventional operations if cyber remains a component of the other services. The long-term implications of keeping cyber a component of other services remain to be seen in terms of recruitment and retention of talent. The lack of an independent cyber service may also affect a government's ability to deliver timely effects in cyberspace, as well as to coordinate operations and carry out deconfliction.

This suggests several avenues for future research:

- How are different states organized and equipped to leverage cyber effects at the tactical and operational levels of war?
- To what extent do limited capabilities and a limited workforce affect the resources that can be leveraged to support strategic and non-strategic initiatives?
- Does the culture of the various services hinder recruitment and retention of cyber talent?
- What are the costs and benefits of creating a cyber service?
- How should buying the hacking of services be taken into account?

Conclusion

Tactical and operational dynamics are the least-studied area of cyberwarfare, despite the fact that cyber conflict is an ongoing reality. This aspect of the field urgently demands greater academic scrutiny due to the stakes involved, as *ad hoc* decisions made at the tactical and operational levels of cyberwarfare are likely to have strategic consequences, both positive and negative. •

Bellovin, Steven M., Susan Landau, and Herbert S. Lin. "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 13, 2016. https://papers.ssrn.com/abstract=2809463.

Chesney, Robert. "Military-Intelligence Convergence and the Law of the Title 10/ Title 50 Debate." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, October 17, 2011. https://papers.ssrn.com/abstract=1945392.

Goldsmith, Jack. "How Cyber Changes the Laws of War." European Journal of International Law 24, no. 1 (February 1, 2013): 129–38. doi:10.1093/ejil/cht004.

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

Kehler, Robert, Herbert S. Lin, and Michael Sulmeyer. "Rules of Engagement for Cyberspace Operations." SSRN Electronic Journal, 2016. doi:10.2139/ssrn.2835633.

Lin, Herbert S. and Taylor Grossman. "The Practical Impact of Classification Regarding Offensive Cyber Operations," forthcoming.

Lin, Herbert S., Kenneth W. Dam, and William A. Owens, editors. Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities. National Academies Press, 2009.

Lin, Herbert S., Kenneth W. Dam, William A. Owens, and Herbert S. Lin, editors. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington, DC: National Academies Press, 2009. http://www.nap.edu/catalog/12651.

Lonergan, Shawn W. "Cooperation Under the Cybersecurity Dilemma" in Confronting Inequality: Wealth, Rights, and Power, edited by Hugh Liebert, Thomas Sherlock, and Cole Pinheiro. New York: Sloan, 2016.

———. "The State and Cyberspace." In Guaranteeing America's Security in the 21st Century. edited by William Parker III. Minneapolis, MN: Mill City Press, 2016.

Long, Austin. "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, June 15, 2016. https://papers.ssrn.com/abstract=2836204.

Valeriano, Brandon and Ryan C. Maness. Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press, 2015.

Bellovin, Steven M., Susan Landau, and Herbert S. Lin. “Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 13, 2016. https://papers.ssrn.com/abstract=2809463.

[Insert more sources]

IMPORTANT WORKS

INTELLIGENCE AND ADVERSARIES

Columbia University	**Moderator: Neal Pollard** **Rapporteur: Justin Key Canfil**
June 16, 2016	

Introduction

The United States Office of Personnel Management (OPM) hack, which was first detected in early 2015 and is estimated to have affected more than twenty-one million Americans[1], has been described as perhaps the most serious breach of US data in the short history of cybersecurity to date[2]. Although the OPM attack has commonly been attributed to China, the US government has so far declined to publicly acknowledge any suspected perpetrators. This episode contrasts with the 2014 indictment of five Chinese People's Liberation Army (PLA) officers by the Western District of Pennsylvania, a US federal court, for alleged cyber espionage. In the PLA Five case, top US officials, including the heads of the Federal Bureau of Investigation (FBI) and Department of Justice (DOJ), respectively, did not hesitate to blame China on the record[3]. John Carlin, assistant attorney general for national security, described the hacks as having occurred "under the shadow of [that] country's flag[4]." Similarly, the FBI openly accused the North Korean state of having conducted a series of computer network attacks against Sony Pictures Entertainment in retaliation for the latter's planned release of a comedy film critical of that country's regime[5].

Why was the United States willing to make public statements alleging attribution in two of these cases but not the third? Is it simply a matter of having sufficient intelligence about the source of the attacks? Does it depend on the extent or nature of

---

1 Zengerle, Patricia, and Megan Cassella. 2015. "Millions More Americans Hit by Government Personnel Data Hack." Reuters, July 9. http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709

2 Barrett, Devlin, Danny Yadron, and Damian Paletta. 2015. "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say." Wall Street Journal, June 5, sec. US. http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

3 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." 2014. Press Release. US Department of Justice Office of Public Affairs. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

4 Id.

5 Nakashima, Ellen. 2014. "U.S. Attributes Sony Attack to North Korea." Washington Post. December 19. https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html.

damage? In the North Korean example, US President Barack Obama told reporters that the United States "will respond proportionally[6]." This chapter will address twin topics–intelligence on cyberattacks themselves and on the adversaries capable of perpetrating them.

The first challenge is recognizing that, in large part, the policy world lacks a theoretical foundation for these concepts. Unlike many other topics, there is a dearth of scholarly literature on intelligence and attribution. While a great amount of theory has been generated within the discipline of computer science, technical practitioners working in the field have generally applied this body of knowledge directly to cases. Comparatively little has made its way to policy audiences or been translated for social scientists. Earlier research on intelligence craft in conventional realms may in some cases be a reasonable analog, but without more of an effort to bridge these two areas we cannot fully deduce the applicability of conventional ideas to cyber intelligence. As one conference participant noted, "Language barriers result in bad decisions and bad laws." Important documents (such as the 1996 IW-D Pentagon report) do exist, but are relatively few in number[7]. Although this report describes only the opinions of the 2016 State of the Field participants, a supplementary bibliography (which participants used in part to inform their discussion) is included in the Appendix for reference.

The second challenge is empirical: attack detection is imperfect and a function of the balance of capabilities between attacker and defender. When network breaches are detected, victims may be reluctant to disclose it for fear of embarrassment and subsequent loss of trust in the organization. Since data is usually proprietary and disclosure often voluntary, this is a problem for good intelligence work, which thrives only when information is available and shared between entities on the same side. The purpose of this chapter is to identify what cyber conflict researchers do know about intelligence and attribution. Once this is identified, the research frontier and policy implications will hopefully become clear.

6 Id.

7 "Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D)." 1996. Washington, D.C: Office of the Undersecretary of Defense for Acquisition and Technology. http://www.au.af.mil/au/awc/awcgate/infowar/iwd/iwdmain.htm.

Definitions

How can we define intelligence, and why is it important? In the simplest sense, "intelligence" refers to information an entity can use when playing strategies against an adversary; namely, information about the adversary's qualities or capabilities[8]. It is critical for effective network defense as well as targeting when defense has failed. Intelligence is systematically collected and processed in order to inform policy options. Beliefs about facts derived from intelligence are rarely certain: intelligence is probabilistic and confidence-based.

Cyber tools can be used to gather intelligence about either cyber or non-cyber attributes, just as it is sometimes possible to glean information about cyber attributes through conventional means. However, the cyber-on-cyber intelligence process represents more than a simple extension of traditional intelligence work, since cyberspace is in many ways unique. Participants disagreed about three corollaries of the definition: first, what the scope of the discussion should be (cyber-on-cyber only, or other forms?[9]). Second, who are the players? While some participants suggested intelligence is an aspect available primarily to the most sophisticated class of actors, such as states, others disagreed, noting that commercial companies, not governments, seem to be doing some of the most advanced intelligence work in cyber conflict. It might be assumed that the emphasis on intelligence is roughly increasing in organizational capacity (which correlates with sophistication), but that this function may sometimes be monotonic and that there may be other variables at play. It should be noted, however, that a multiplicity of cyber actors use the same types of tools and techniques; as a result, our state-centric view covers only one possible type. One justification is that the conference was concerned with cyber conflict. The most sophisticated nonstate actors in cyberspace are generally understood to be motivated by criminal ends. This is of course a simplification, but one made for purposes of tractability.

8 Definition proposed by a conference participant, for which we observed relative consensus.

9 The manner in which conventional intelligence informs cyber operations is a particularly interesting area of inquiry. For instance, compared to intelligence about physical targets gleaned through cyber operations, do traditional operatives or analysts have a greater tendency to miss valuable cyber intelligence because of the technical demands in knowing what to look for? Perhaps an analogy could be made to nuclear intelligence, although pieces of cyber intelligence might be more ubiquitous and their discovery more ancillary.

Figure 1.

Scope of 2016 Panel Discussion

Spectrum of Activity		
Cyber Only	Cyber & Physical	
		Operational Nature
●	○	Purely Informational
○	○	Clandestine and Covert

Third, participants debated whether the definition should deal purely with informational aspects, or whether the conception of cyber intelligence should also include covert activities (requiring high-level approval) or clandestine (not requiring high-level approval, but taken in the course of information collection). Related to these is the concept of counterintelligence. Counterintelligence is particularly relevant to cyber conflict for both state and nonstate actors. As several participants noted, the same case officers may "wear multiple hats" working for instance both in counterintelligence and covert action (although there is a large degree of role specialization[10]). To the extent that this overlapping activity occurs, it makes dichotomizing purely informational work from other aspects problematic. In the interest of moving forward with first steps at the 2016 State of the Field conference, participants settled on a discussion of state-based and primarily informational intelligence processes, leaving other facets of the definition for potential future consideration.

Attribution, on the other hand, was defined as beliefs about the actor on the other end of an exchange; that is, knowledge about an adversary's identity. This is principally relevant for defenders seeking to trace their attackers. Also confidence-based and probabilistic, reliable attribution is critical for effective response in the event of an attack (e.g. strategic deterrence, law enforcement, and countermeasures). Intelligence and attribution play related roles: intelligence aids attribution, but each serves a separate purpose. Under the 2016 panel's definition, intelligence is proactive, informing threat assessment and bolstering operational capability (both offensive and defensive). Attribution, conversely, is reactive, typically coming into play only after an attack has been enacted and detected. Both serve to inform political action.

10 Specialization carries additional cost and organizational capacity requirements. If specialization leads to better intelligence, this may suggest that intelligence is indeed the privileged tool of highly complex players such as states.

Mapping "Intelligence"

Within strategic dynamics, intelligence is extremely important. While Sun Tzu advises "know thy enemy[11]," Clausewitz points to the concept of friction: "Everything is very simple in war, but the simplest thing is difficult[12]." Intelligence analysis addresses both prescriptions by helping decisionmakers account for uncertainties[13].

Participants noted that intelligence may operate on four different levels: tactical, operational, strategic, or political. The political level is about what another actor may intend to do; the other levels are about what he/she has the ability to do and how to best counter this. Because these levels are more central to a discussion of policy formulation or strategic dynamics, the Intelligence and Adversaries panel did not dwell long on them: the key takeaway for participants is that the purpose of intelligence is to provide leadership with information on these dimensions. Second, intelligence may have three "types" or orientations: information gathering, threat warning and assessment, and damage assessment. First, intelligence aimed at gathering information about an adversary might encompass his/her weak points, centers of gravity, and capabilities. Here, information is gathered in three categories: operating environment, adversary, and that adversary's likely course of action. Second, intelligence can feed into threat warning and assessment, providing information about the level of risk, both in terms of defensive vulnerabilities and adversary capabilities. Third, intelligence plays a role in damage assessment: how effective are operations in influencing an adversary and/or how much damage has that adversary done?

11 Ames, Roger T., trans. 1993. Sun Tzu: The Art of Warfare. 1st edition. New York: Ballantine Books.

12 Clausewitz, Carl von. 1989. On War, Indexed Edition. Translated by Michael Eliot Howard and Peter Paret. Reprint edition. Princeton, N.J.: Princeton University Press.

13 Sun Tzu also wrote, "The general who wins a battle makes many calculations in his temple before the battle is fought. The general who loses a battle makes but a few calculations beforehand. Thus many calculations lead to victory and few calculations to defeat. It is by attention to this point that I can foresee who is likely to win or lose" (as quoted in Joint Publication 6-12, supra).

Intelligence is also understood to have a seven-step lifecycle: (1) formulation of informational needs, (2) data collection, (3) data processing/exploitation, (4) analysis, (5) dissemination, (6) consumption, and (7) organizational feedback[14].

How Cyber Intelligence is No Different

Participants achieved consensus readily on the following points:

- This lifecycle framework is the same in cyber conflict, although being good at them is another question. Whether these steps are appropriate for cyber and how to get better at following them represent interesting areas for academic research and program evaluation.

- Many of the tools and tactics are the same: for example, attempts to "flip" enemy agents or infiltrate their networks, as demonstrated in the FBI's takedown of hacktivist group Lulzsec[15].

- At least in the United States, clandestine and analysis roles are blurrier in cyber than in traditional spaces. Specifically, Title 10, Title 18, and Title 50 operatives are said to be "triple-hatting" as the United States blends both military and classic intelligence functions (often facetiously termed "Title 78"). One participant likened it to equipping U-2 Dragon Ladies—high-altitude spy planes used by the US Air Force since the late 1950s—with JDAMs (Joint Direct Attack Munitions, or "smart bombs"). Another analogy might be remotely piloted aircraft (drones): although the technology to arm unmanned reconnaissance platforms existed for many years prior to the MQ-1 Predator, there was said to have been considerable hesitation in policy circles about whether the United States would be justified in doing so. This mirrored a common progression, as most weapons platforms began as reconnaissance platforms. Today there is arguably no legal prohibition on equipping military-grade drones with explosive ordnance, although many still disagree on moral or political

14 These seven steps are often collapsed into a smaller number; the State of the Field panel treated them as separate and discrete. Whether nonstate entities employ a similar life cycle is an open question.

15 Kopstein, Joshua. 2014. "How an FBI Informant Orchestrated LulzSec's Hacking Spree." The Daily Beast. June 6. http://www.thedailybeast.com/articles/2014/06/06/how-an-fbi-informant-orchestrated-lulzsec-s-hacking-spree.html.

grounds. Similarly, State of the Field participants disagreed about whether weaponizing platforms is legal or appropriate in the context of cyberspace[16]. At least one participant advanced the notion that developments in contemporary international relations mean compartmentalized functionalities are obsolete, in much the same way that narcoterrorism revolutionized law enforcement.

- Many participants theorized that considerably more intelligence is needed to take action in cyberspace than in conventional dimensions. For instance, the authors of the Stuxnet malware had to know quite a lot about the particular centrifuge models their program was intended to disable. Some of the more technical participants questioned this idea, hinting that research opportunities exist to further synthesize what computer science experts know can be done with what policy experts know is needed in a typical operation.

- Although intelligence is often regarded as a pacifying force in the study of international relations since it mitigates mutual fears about vulnerability, clarifies or resolves misperceptions about relative strength or intentions, and otherwise solves problems related to private information, this tendency is complicated in the realm of cyber conflict. First, based on who is affected: since a variety of players (including private actors) share network infrastructure, the potential for collateral damage is endemic. Second, intelligence collection in cyberspace is very often hard to distinguish from the precursor to an attack, since both involve network intrusion. Clarifying which is which can be costly and time-consuming, meaning determinations about proportional response must sometimes be made without this information inside windows of vulnerability and under conditions of extreme uncertainty. This has adverse implications for deterrence and escalation.

- The use of civilian infrastructure seems to be much more common in cyber. For instance, one participant noted that Stuxnet was accomplished using falsified Microsoft certificates. According to this participant, the moral and legal obstacles to having an operative pose as a Microsoft technician in real life are higher.

16 It should be pointed out, however, that unlike drones, however, there seems to have been much less hesitation to merge camera and gun in the cyber context.

Participants raised the point but could not agree where the line between military and civilian infrastructure should be drawn or where it is being drawn in practice. This issue strikes at the heart of a policy priority for the US government: the diffusion of the norm against economic espionage. The dual-use nature of cyber infrastructure, coupled with the interconnectedness of a multitude of actors, might mean that disentangling "economic" from "strategic" intelligence craft might be more difficult than it is in traditional spaces. This only intensifies the difficulty of making practical distinctions between intelligence collection and covert action, a problem that one participant argued "goes back to the founding of the [US] republic." Another complication is that to a large degree these same intelligence tools are available to nonstate actors, including private companies who might wish to use them to gain an economic edge. These elements hint that economic actors will play a much more central (and autonomous) role in cyber conflict than previously envisioned.

Mapping "Attribution"

The great irony is that, although cyberspace is literally constituted by a superabundance of data, attribution in the domain is considered inherently difficult and anonymity easy to maintain[17]. This is one of the most common motifs in the cyber conflict literature. It is true that detection and differentiation are systematically problematic. Yet despite the conventional wisdom and known difficulties, attribution is possible: "there really is a smoking gun[18]," as successful past indictments show[19]. The difficulty of attribution is a "fixation," according to Jason Healey, who argues it is often merely a mental trap[20]. There was widespread agreement among participants on

17 "Joint Publication 3-12 (R): Cyberspace Operations." 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. Web. See also Libicki, Martin C. 2009. "Cyberdeterrence and Cyberwar." RAND Corporation.

18 1996 Defense Science Board Report, supra.

19 e.g. Mitnick, Kevin, Steve Wozniak, and William L. Simon. 2012. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. New York: Back Bay Books.

20 Healey, Jason. 2012. "Beyond Attribution: Seeking National Responsibility in Cyberspace." Atlantic Council. February 22. http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.

Figure 2.

Why Attribution is Important

Purpose	Description
Insurance Claims	Valuable for prevention, risk management strategies
Law Enforcement	Must identify perpetrators beyond a reasonable doubt (in domestic context)
Deterrence	Effective deterrence requires the ability to selectively punich violators
Countermeasures	Coercive/retailatory instruments must clearly link punishment with noncompliance

this view. Because so much of the cyber conflict literature is based on the premise that attribution is hard (or impossible), many of our theories may need revisiting[21].

How is attribution accomplished? The short answer is through technical network forensics. When an attack occurs, digital footprints can be traced from the scene of the crime. Yet, as participants recognized, there is an important qualitative difference between (1) identifying the machine from which an attack appears to have originated (although it may have been routed through several others on its way to the target), (2) identifying the person behind the keyboard of the actual computer used to launch the attack and the country in which it is located, and (3) determining whether a higher authority is responsible for ordering the attack. A number of creative techniques have been devised to parse these differences. Attack indicators can be generally placed in one of three categories:

- Indicators of Compromise (IOCs): technical details; digital footprints[22]

21 Distributed Cloud Delivery Networks and totalitarian government may also be systematically squeezing anonymity out of the internet for private actors. See Schneier, Bruce. 2013. "The Battle for Power on the Internet." The Atlantic, October 24. http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

22 Denning, Dorothy E. 1999. Information Warfare and Security. Essex, UK, UK: Addison-Wesley Longman Ltd; Andress, Jason. 2015. "Working with Indicators of Compromise." ISSA. https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0515.pdf.

- Tactics, Techniques, and Procedures (TTPs): observations about behavior consistent with that of known adversaries (not necessarily digital, but observed digitally[23]). This could include whether attack patterns appear to correlate with religious holidays, particular working hours, or, in the case of states, foreign policy priorities.

- Human Intelligence (intelligence gathered non-digitally)

Techniques have become increasing sophisticated in recent years. Cyber forensics has moved from its reliance on isolated IOCs in the late 1990s, to incredibly detailed iterated pattern analysis based on TTPs, to machine learning algorithms and "kill chain modeling[24]," to diplomatic indices[25]. Ideally, attribution is based on repeated observation, matching IOCs with TTPs and supplementing with diplomatic factors or human intelligence[26]. In practice, however, these methods take time and are resource-intensive. It may be the case that targets (particularly governments in time-sensitive instances) sometimes consider imperfect or partial attribution as "good enough," relying on rudimentary *cui bono* (who benefits?) tests[27]. One problem noted by the participants is that there is no agreed-upon standard of evidence; the burden of proof varies with the preferred response option, but the preferred response ought to depend on what is known about the attack. Because evidence is endogenous to retaliation in this way, inference problems abound. Second, depending on what the

---

23 "Tactical Cyber Intelligence." 2015. Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force. http://www.insaonline.org/i/d/a/b/TacticalCyber.aspx.

24 Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1 (2011): 80.

25 Healey, Jason. 2011. "The Spectrum of National Responsibility for Cyberattacks." Brown Journal of International Affairs. https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/18.1_Healey.pdf.

26 A minority of participants disagreed with the word choice of "ideal" or "sophisticated," preferring to describe these techniques as merely the most "common."

27 n.b. Libicki, supra) cautions us against overreliance on *cui bono* tests, which are not proof, can create new enemies when improperly applied, and may inadvertently implicate innocent parties.

accepted threshold is, how can lower-capability victims meet it? Articulating universal standards for evidence is an avenue for much-needed future research–the task of the legal panel.

Given what we know about attribution, exactly how easy or reliable does it seem to be? One participant voiced the refrain that attack is easy in cyberspace because "defense has to be right 100 percent of the time, but offense needs only to be right once." On the subject of attribution, however, the participant argued that the situation is actually reversed. While perhaps this is true, it is far from satisfying. The relationship between offense and defense in the former statement is often said to mean that offense is "dominant" (in other words, that it is the more cost-effective of the two). Can attribution really be said to be dominant over anonymity, however, if attackers are identified correctly in only one out of several hundred attacks?

Participants raised a separate caveat, noting that "prompt" attribution is still difficult.[28] Attribution is expedited when the victim is already in the adversary's networks, though of course this can work both ways. Participants were divided over whether the lack of promptness has practical implications for deterrence[29]. The majority, however, was of the opinion that attribution ease decreases in parallel with attack intensity. Specifically, passive attacks (diversions, interceptions) are much harder to trace than *bona fide* "attacks" that manipulate data or degrade capabilities, especially as the timeline extends.

These aspects illustrate that attribution technology is an incredibly powerful tool but that it can also be misused[30]. The data may be well mapped, but effective attribution still requires enhanced algorithmic models and humans in the loop. Similarly, although

---

28 Of course, what counts as "prompt" is debatable.

29 At least in terms of international law, it does (see Damrosch, Lori, Louis Henkin, Sean Murphy, and Hans Smit. 2009. International Law, Cases and Materials, 5th edition. St. Paul, Minn: West). Immediacy may also be required for self-defense purposes: for example, in the classic and incredibly prescient fictional movie WarGames (1983), North American Aerospace Defense Command (NORAD) is placed on high alert after teenager David (Matthew Broderick) accidentally hacks into a military mainframe and triggers a simulation. Had the US military initially attributed the hack to a kid from the suburbs, the countdown to World War III might have been avoided.

30 To say nothing of civil liberties concerns, which although merits discussion is a highly politicized subject that lies beyond the scope of this chapter.

cyberattacks are launched through computers, it is important to remember that there are humans on both ends. As a result, much can be learned through studying human behavior and human error (although inferences can also be biased or corrupted on the receiving end, as well). Suspicions are easy to confirm, but victims may only be on the lookout for confirmatory evidence while conveniently overlooking or ignoring contradictory information. This can lead to what statisticians call "Type II" errors–false positives–as victims search for someone to blame.

Moving Forward

Intelligence

Does existing theory on this topic take intelligence for granted? Per the Clausewitz quote *supra*, we know that things rarely go exactly according to plan in conflict–perhaps even less so in cyber conflict, where interconnectedness and heightened uncertainty make consequences unpredictable. Although it may be possible to theorize about how intelligence works and confers advantages under ideal conditions, the intelligence life cycle may work more slowly or overlook critical pieces of information, since adversaries in cyberspace are potentially stealthier. A full-fledged study (and not just a white paper) on how cyber intelligence *per se* works is very much needed, although for reasons of secrecy it may be difficult to execute such a project. In the meantime, scholarly research ought to focus more on how cyber methods differ from those of traditional intelligence craft. The first priority should be confirming that the life cycle outlined above indeed reflects practice, yet there has been little discussion devoted to this question (even in Joint Publication 3-12, which deals expressly with several aspects). Participants shared full consensus on this point.

Another challenge is that most of what we think we know is Western-centric and introspective, yet cross-national context is paramount. Participants agreed with this point, but were divided over where the comparison ought to be drawn. Among various aspects, such as a host country's institutions, organizational tendencies, culture, ideological salience, religious background, the cognitive aspects of its leaders or hackers, its international relationships, normative subscriptions, legal doctrine, and so on, which are most important for understanding behavior, and do they influence behavior differently in cyberspace?

It may be worth exploring perception about effects to a greater degree, as well: damage assessment is in many ways easier in the physical world. For instance, a bomb crater is visible to the naked eye and can be spotted with a reconnaissance flyover or

satellite. Returning to a hostile network to assess cyber damage is less often feasible. Being confident about having completely analyzed the damage to one's own systems in the wake of an attack is also a challenging proposition. How do we understand what we have accomplished? How does the adversary? How do they understand what we understand, and vice versa?

A final point is how to best define "economic espionage." The difficulties therein have already been discussed *supra*, but the magnitude of this problem merits mentioning it again. For example, the following hypothetical was posed for the participants: an unnamed state steals radar technology and distributes it to national companies to build better stealth capabilites for military use. A plurality of participants agreed that this constitutes a legitimate (if not strictly legal) act because it serves national defense purposes. When the state was instead said to have stolen the technology in order to sell it on the market, however, participants were more inclined to call this economic espionage. Individual participants raised several possibilities. For instance, perhaps it depends on whether the receiving company exports the technology or sell it only to the state's military. Or perhaps it depends on whether the company sells the technology itself rather than simply equipment produced with it. Maybe it also depends on whether the technology is an innovation that is later adapted to commercial purposes for profit or is of a dual-use nature to begin with. Some were uncomfortable with any allowances, arguing that espionage with any ramifications for commercial activity represented a form of neo-mercantilism. Again, as with the above issues, this might also be a culture- or society-specific concern requiring better international dialogue instead of punitive rules or threats.

Attribution

The discussion yielded several conclusions for attribution and adversaries, too. Participants felt that attackers and defenders are both getting smarter. Although it remains to be seen whether attribution technology will eventually outpace attackers' ability to hide, the evidence thus far suggests that forensic ability is keeping pace. Knowing who was behind an attack may never be perfectly certain, but the ability to make educated guesses allows states to hold their attackers responsible. However, whether responsibility leads to accountability is another question: the requisite degree of confidence depends on the response one wishes to adopt, which is of course contingent on one's ability to execute that response. Furthermore, the amount of evidence necessary to convince defenders may not be sufficient to persuade others. Finally, the burden of proof under *lex lata* in international law may not even be obtainable for common attacks (see Chapter 6 in this same volume).

Although security researchers are professionals, attribution and decisionmaking (especially in time-sensitive environments) may be hampered by cognitive and motivational biases, path dependence or outmoded standard operating procedures, biological factors, emotions and affectations, imperfect information, or stress[31] [32] [33] [34]. An enormous body of political science and political psychology literature deals with these factors. We know little about how they operate in cyber conflict as opposed to conventional conflict, but the shortening of the time horizon, heightened technical complexity, and maximization of the uncertainty condition predicts that sound decisionmaking might actually be more difficult[35].

A number of participants believed that making the leap from immediate perpetrators to responsible parties is something with which technical indicators struggle. Healey's work offers some solutions to defenders themselves who can use his framework to make policy choices, but the burden of proof problem is still in many ways in the eye of the beholder for international audiences and international law[36]. The majority disagreed with this assessment, arguing, for instance, that experiences in recent years have confirmed all our suspicions. However, the threat of false positives is real. Similarly, our beliefs about who our adversaries are may be self-reinforcing; we should want to be able to recognize changes in adversaries' policies when they do occur. While current attribution technologies can be sufficient to impugn attackers, the need for clearer and universal standards of evidence is indisputable. Until this point is resolved, countries will continue to operate based on disparate perceptions about the permissibility of attack and response.

---

31 Jervis, Robert L. 1970. The Logic of Images in International Relations. Reissue edition. New York, N.Y.: Columbia University Press.

32 Mercer, Jonathan. 2013. "Emotion and Strategy in the Korean War." International Organization 67 (2): 221–52.

33 McDermott, Rose. 2004. Political Psychology in International Relations. University of Michigan Press.

34 Yarhi-Milo, Keren. 2014. Knowing the Adversary. Princeton University Press.

35 One participant also suggested "hangovers" be added to the list.

36 Id, 2011.

Attacker motivations (political vs. criminal vs. pranksterism) are unobservable and can only be inferred, yet they are crucial for determining the source and formulating an appropriate response. If motives can only be inferred and not directly observed, are they really a useful indicator or simply a proxy for other indicators[37]? Judgments can be biased either when one's analysis is flawed or when the information used to derive the analysis is incorrect or incomplete. Advanced techniques (which break the reliance on isolated IOCs and *cui bono* tests) help defenders avoid the pitfalls of bias, but crucially, they hinge on repeated observation (and detection in the first place). Until the learning process converges on a likely suspect, attackers act with impunity. In this regard, defense and risk management strategies are paramount as first lines of defense. Learning can be sped up through information-sharing procedures, something the US Department of Homeland Security and others have strongly advocated in recent years[38], although private-public sector cooperation hinges also on trust (a constant tension[39]). The movement especially among private companies away from static defense and toward active prevention ("anticipatory intelligence") has arguably yielded only mixed results[40]. On a more optimistic note, although isolated attacks may carry the advantage from an attribution standpoint, they tend to be less operationally effective for aggressors. When attacks are severe, they are likelier to be part of pervasive campaigns, in which case the perpetrators are likelier to be identified (all else equal).

37 Or inherent beliefs, when not backed by any evidence.

38 https://www.dhs.gov/topic/cybersecurity-information-sharing

39 For examples, see Lillington, Karlin. 2015. "Microsoft Irish Data Case Raises Critical Issues for Cloud Computing." The Irish Times. April 23. http://www.irishtimes.com/business/technology/microsoft-irish-data-case-raises-critical-issues-for-cloud-computing-1.2186247; Selyukh, Alina, and Camila Domonoske. 2016. "Apple, The FBI And iPhone Encryption: A Look At What's At Stake." NPR.org. February 17, 2016. http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake.

40 "Operational Levels of Cyber Intelligence." 2013. Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force. http://www.insaonline.org/i/d/a/Resources/CyberIntel_WP.aspx; Perlroth, Nicole. 2016. "The Chinese Hackers in the Back Office." The New York Times, June 11. http://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html. Several participants from this sector pushed back against this argument, although it was unclear whether they were in the minority or majority.

The last step in the intelligence life cycle, "feedback," is also missing. Because we cannot know how poor intelligence was in the early days of cyber conflict, it is hard to know whether states have improved. One participant asked, for example, whether the famous Rose Garden agreement between Chinese President Xi and US President Obama has led to better outcomes or whether, if China is responsible for hacking the United States, it has simply gotten better at hiding it[41]. The movement toward greater levels of information sharing may provide a basis for evaluation moving forward. For instance, if the private sector begins to disclose more breaches, the US government can better estimate the proportion of attacks that it failed to detect and thwart independently. Lastly, this criticism may not be unique to cyber.

Conclusion

Participants were also able to reach consensus fairly easy on many of the major points, suggesting that although little documentary research is available to date, a coherent body of knowledge is alive in the minds of expert practitioners and scholars. The downside, of course, is that this body of knowledge still has numerous gaps. The twin topics of intelligence and attribution still lack common definitions, a taxonomy, and universally-recognized standards[42]. This is perhaps the most important near-term task for researchers and policymakers.

Another question is how much the field has grown over the years. Many of the most important documents on these topics were written in the 1990s. Are key ideas really so constant in cyber intelligence, or are our theories in need of an update? Certainly we may be in need of institutional innovation: intelligence needs are seen by some to be outpacing intelligence organizations authorities, as evidenced from the "Title 78" discussion.

Also missing (in addition to those items portrayed in Figure 1) is a discussion on threat warning capabilities as a tactical concept (differentiated from threat assessment, which deals with a more preventative and strategic outlook). How like

41 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference." 2015. Whitehouse.gov. September 25. https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

42 Although c.f. Defense Science Board Report (IW-D), 1996, supra

conventional spaces is threat warning in cyberspace? Are there lessons to be learned from the nuclear age, or is cyber conflict too unique[43]?

Some participants were careful to point out that a considerable amount of data has been pooling for some time now at consulting and insurance firms. We may be growing closer to a world in which attack data is less proprietary and more available, which would be a boon for both scholars and analysts. This raises the question, however, of where such data should be "racked and stacked." Who should be responsible for maintaining it? Who should be granted access? Who will decide these issues?

Finally, when thinking about attribution, how should we think about the role of the private sector? Does the proliferation of cybersecurity research and consulting firms indicate that government has fallen short on its commitment to assist private actors, or is it a consciously more efficient way of delegating the task to a set of agents with deeper expertise? Or, in some places perhaps, is it hacking for hire–the modern equivalent of a Letter of Marque? Is this optimal, and if so why? In an international context, how far should these entities be allowed to go to protect client interests? Most germane to our discussion, what sort of authority does the private sector have to make attributions and what are the political implications for governments? These questions, although relevant to attribution, may be better left to the law panel in future conferences.

Operationally, intelligence and attribution is "messier" in cyberspace. Intelligence is accustomed to being an art, a craft. The technical parameters of cyberspace put pressure on it to become a science, but the nuance of politics is lost in science. Politically, these issues are also messier: the dual-use nature of cyber infrastructure means economic espionage is no longer cleanly compartmentalized from more "legitimate" forms of spying, with adverse implications for the growth of international norms as well as the risk of escalation in crises. In many ways, however, the cyber process resembles traditional intelligence work. This yields a promising starting point. Our task now must be to deduce how cyberspace skews predicted outcomes. The Intelligence & Adversaries panel at the 2016 State of the Field conference succeeded in mining some of the most important topics in these areas, but many more opportunities for research exist. •

43 A parallel explored at length by Herb Lin in several 2014-2016 talks.

Anders, E.R. “Mike.” “Activity Based Intelligence (ABI) and the Cyber Domain.” Cyber Intelligence Blog, June 25, 2016. https://cyberintelblog.wordpress.com/.

Andress, Jason. “Working with Indicators of Compromise.” ISSA Journal, 13, no. 5 (May 2015): 14–20. 5/15. https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0515.pdf.

“APT1: Exposing One of China’s Cyber Espionage Units.” Mandiant, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Andrews, Duane. “Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D).” Washington, DC: Defense Science Board, November 1996. http://www.dtic.mil/get-tr-doc/pdf?AD= ADA319571.

Arquilla, John, and Douglas A. Borer, editors. Information Strategy and Warfare: A Guide to Theory and Practice. 1st edition. Routledge, 2007.

Cappelli, Dawn M., Andrew P. Moore, and Randall F. Trzeciak. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. 1st edition. Upper Saddle River, NJ: Addison-Wesley Professional, 2012.

Chesney, Robert M. “Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate.” Journal of National Security Law & Policy 5 (February 9, 2012): 539. , 2012. http://jnslp.com/wp-content/uploads/2012/01/Military-Intelligence-Convergence-and-the-Law-of-the-Title-10Title-50-Debate.pdf.

“Cyber Intelligence - Setting the Landscape for an Emerging Discipline.” Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force, 9/September 2011. http://www.insaonline.org/i/d/a/Resources/Cyber_Intelligence.aspx.

Denning, Dorothy E. Information Warfare and Security. 1st edition. New York : Reading, Ma: Addison-Wesley Professional, 1998.

Devost, Matthew G. “Cyber Adversary Characterization.” Blackhat USA, 2003. https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf.

Devost, Matthew G., Brian K. Houghton, and Neal Allen Pollard. “Information Terrorism: Political Violence in the Information Age.” Terrorism and Political Violence 9, no. 1 (March 1, 1997): 72–83. doi:10.1080/09546559708427387.

Ellis, James, David Fisher, Thomas A. Longstaff, Linda Pesante, and Richard D. Pethia. “Report to the

President's Commission on Critical Infrastructure Protection." Software Engineering Institute, January 1997.

Gourley, Bob. The Cyber Threat, 2014n.d.

"Guide for Conducting Risk Assessments." National Institute of Standards and Technology (NIST), US Department of Commerce, September 209/12. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Healey, Jason. "Beyond Attribution: Seeking National Responsibility in Cyberspace." Atlantic Council, October 17, 2016. http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.

Healey, Jason, and Karl Grindal, editors. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Vienna, VA: Cyber Conflict Studies Association, 2013.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Lockheed Martin Corporation, 2010. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

"Joint Publication 2-01, Joint and National Intelligence Support to Military Operations.," January 5, 2012. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf.

"Joint Publication 3-12, Cyberspace Operations.," February 5, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

"Joint Publication 3-13, Information Operations.," November 20, 2014. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

"Joint Publication 3-60, Joint Targeting," January 31, 2013. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm.

Libicki, Martin C. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009.

"Operational Levels of Cyber Intelligence." Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force, 9/September 2013. https://www.insaonline.org/CMDownload.aspx?ContentKey=cfdfcf7c-02b4-4507-a054-2606d684ffb0&ContentItemKey=bc0f998f-85f7-4db6-9288-903f748e1de9.

Parker, Tom, Marcus Sachs, Eric Shaw, Ed Stroz, and Matthew G. Devost. Cyber Adversary Characterization: Auditing the Hacker Mind. 1st edition. Rockland, MA: Syngress, 2004.

Perlroth, Nicole. "The Chinese Hackers in the Back Office." The New York Times, June 11, 2016. http://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html.

Poznansky, Michael, and Evan Perkoski. "Clandestine or Covert? Rethinking Secrecy in Cyberspace." Working paper, September 7, 2016. https://papers.ssrn.com/abstract=2836087.

Rattray, Gregory J. Strategic Warfare in Cyberspace. 1st edition. Cambridge, MassMA: The MIT Press, 2001.

"Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)." Washington, DC: Defense Science Board, November 1996.

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

Stoll, Cliff. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Reissue edition. New York: Pocket Books, 2005.

"Tactical Cyber Intelligence." Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force, 12/December 2015. http://www.insaonline.org/i/d/a/b/TacticalCyber.aspx.

THE STRATEGIC DYNAMICS OF CYBER CONFLICT

Columbia University	**Rapporteur: Erica D. Borghard** **Moderator: James Mulvenon**
June 16, 2016	

Introduction

Strategy is a critical element of statecraft. It is at the intersection of national policy and the operational and tactical levels of warfare. Outcomes at the strategic level are decisive and can spell victory or defeat for governments. Despite the clear importance of strategy, the scholarly literature on the strategic dynamics of cyber conflict is still emerging. Furthermore, policymakers have yet to agree on key strategic principles for the use of cyber power. Therefore, this chapter identifies four key issues: the nature of power in cyberspace; deterrence and compellence; attribution and the implications of having multiple actors operating in this domain; and achieving strategic stability in cyberspace.

Power

The central question of power, put simply, is: power over whom, and for what purpose? Despite the apparent simplicity of this question, there has been a longstanding debate in the traditional international relations literature regarding definitions of the nature of power, as well as how it should be measured. In realist terms, state power is defined solely in terms of military power (i.e., the capabilities associated with the organized use of force to deny, deter, coerce, or swagger). However, even in this realm there are debates regarding how military power should be defined, in particular, whether military power should be conceived of as a quantitative metric that reflects a state's objective warfighting capabilities (e.g., manpower, material, industrial base, etc.), or whether qualitative measures of military power that center on force employment, doctrine, and strategic culture (which, of course, are more difficult to measure) merit inclusion.

Critics of the exclusive focus on military power counter that other aspects of power, such as economic power, diplomatic power, informational power, and soft power, are as important—if not more important—than military power. This debate has become particularly salient in the wake of the fall of the Soviet Union and the alleged irrelevance of traditional conceptions of power and arguments about the futility of using military power to achieve political objectives.

There have also been debates in the international relations literature regarding whether power, regardless of its conception in military or non-military terms, is a relative concept (i.e., power is only relevant vis-à-vis another actor) or an absolute one. This distinction is linked to the debate surrounding absolute versus relative gains.

The concept of power in cyberspace remains contested. In many ways, these debates mirror debates in the conventional realm, namely, whether cyber power should be conceived of primarily in military terms—the capabilities associated with launching coercive campaigns to punish an adversary and impose one's will—or in economic, diplomatic, or informational terms. The latter group conceptualizes cyber power in terms of the capabilities associated with attaining access for the purposes of gaining information to exploit an economic or bargaining advantage.

Measuring cyber capabilities is also incredibly challenging. In terms of absolute capabilities, it is difficult to develop a near-universal metric due to the unique nature of each target and the corresponding uniqueness of the cyber tool that must be developed to access and exploit it. In sharp contrast to nuclear warfare, cyber conflict does not have the luxury of the predictable, repeatable effects associated with the physics of nuclear detonations, and must factor in the specific attack surface and vulnerabilities of the target network to assess the success or failure of an attack. Metrics that may be relevant for this domain are also wide in scope, to include software and hardware development and the technical skill of a state's workforce. Moreover, there are debates regarding whether quantitative metrics are more important than qualitative ones. The relevance of one type of metric versus another will largely depend on the objective at stake in the use of cyber power. In terms of relative capabilities, assessing relative strength in cyber space is also problematic given that many capabilities are custom-tailored to a particular target system, and that these capabilities often have a shelf life because they rely on access to vulnerabilities that could be patched by the time they need to be exploited.

Similar to debates in the conventional literature regarding the decisiveness of any given capability (most notably, discussions surrounding whether air power alone can achieve decisive political outcomes, or whether this capability is only useful in conjunction with ground forces), there has been considerable discussion regarding cyber power's utility as an independent instrument of state power. Some cyber power enthusiasts have claimed that states can use cyber means alone to achieve decisive outcomes in warfare; however, the prevailing consensus is that cyber means are most useful in tandem with conventional ones. This is due to the simple fact that it is difficult to impose sufficiently high costs on an adversary to force a decisive concession. Unlike conventional munitions, which destroy whatever target they hit, there is no universal lethality of cyber weaponry—the latter must be tailored to specific targets. Moreover, the planning that would need to go into a cyber campaign is tremendous and, at this point in the evolution of cyberwarfare, poses significant developmental and testing costs. Of course, this is liable to change in the future if the interdependence of networks continues to progress at its current rate and the Internet of Things

becomes more of a reality, because this would create more vulnerabilities with fewer redundancies.

The above discussion suggests several critical research questions that illuminate key aspects of the nature of cyber power:

- How is power defined in the state system and how might definitions of cyber power overlap with and differ from them?
- Is cyber power primarily useful as a relative or an absolute concept?
- Does cyber power have an independent military utility, or is it primarily a tool of information warfare?
- How useful are other frameworks, such as those pertaining to chemical, biological, and nuclear capabilities, for understanding the nature and applicability of cyber power?
- How might the evolving nature of cyberwarfare change existing assumptions about its dynamics?

Deterrence and Compellence

Coercion, as distinct from brute force, is the manipulation of threats and incentives to change an adversary's behavior through changing her calculations about the costs and benefits of particular courses of action. Thomas Schelling distinguishes between two types of coercion: deterrence and compellence (typically, other scholars use coercion and compellence interchangeably).

Deterrence at its core is fundamentally status quo-oriented—it threatens to impose costs on an adversary in excess of the target's valuation of the objective it seeks to achieve if the target alters its behavior in a manner the deterring state finds objectionable. Deterrence succeeds if nothing changes and the prevailing status quo remains. Deterrence can be achieved through two means: denial (where a state prevents an adversary from taking action against it through convincing the latter that it will surely be defeated or incur unpalatable costs in her attempt to surmount the deterring state's defenses) and punishment (where a state threatens to impose immeasurable pain and suffering on an adversary's civilian population and society).

The literature on deterrence has been most developed in the context of nuclear weapons. This literature grappled with two interrelated questions, particularly from the perspective of US foreign policy and grand strategy. First, how could the United States deter a Soviet conventional assault against Western Europe, where the latter had a conventional advantage? Second, assuming the answer to the first question was a policy of first use of nuclear weapons, how could mutual nuclear deterrence be

achieved such that the two nuclear-armed superpowers could avoid a civilization-ending nuclear exchange? These two questions also point to the distinction between direct and extended deterrence, with the latter focused on deterring an adversary from attacking an ally by claiming that the allies' interests are just as integral as one's own.

Central to deterrence, particularly nuclear deterrence, is the notion of credibility. The efficacy of the US nuclear umbrella relied on credibility—the extent to which the target believes the United States will escalate to nuclear warfare in defense of its allies' interests. So too, the stability that followed from mutually assured destruction relied on each side believing that the other was really crazy enough to risk nuclear war to achieve a given political objective—the gains of which would surely be outweighed by the costs of achieving it. Academics and policymakers, therefore, sought to find ways to enhance the credibility of a deterrent threat. These methods included trip-wire forces, engaging in brinksmanship, the so-called "madman theory," automaticity, and other means that eliminated the flexibility of the deterring state.

There is also a relatively small literature on conventional deterrence, which is more focused on deterrence through denial. Nuclear weapons made deterrence through denial irrelevant, because they enabled a state to inflict pain and suffering on an enemy population while bypassing its armed forces.

In contrast, compellence involves issuing threats or the limited application of force to change an adversary's behavior. It is generally assumed that compellence is harder to achieve than deterrence because of the very public and observable nature of the concession, which leads the target to lose face (deterrence is harder to observe). Indeed, empirical literature has demonstrated that successful militarized compellent threats are few and far between. A significant literature has also developed around the utility of air power as a tool of compellence. However, strong divides remain regarding its effectiveness.

In the cyber domain, much of the debate among academics has been focused on whether it is possible to deter unwanted actions in cyberspace, and whether this is most likely to be achieved through a denial or a spunishment strategy. There are three issues related to deterrence in cyberspace: whether cyber means can be used to deter unwanted action in cyberspace; whether cyber means can be used to deter unwanted action in conventional domains; and whether conventional means can be used to deter unwanted action in cyberspace. The literature has primarily focused on how to deter unwanted actions in cyberspace without disaggregating the three issues above. Therefore, while the prevailing consensus regarding deterrence in cyberspace is that it is incredibly difficult to achieve, its difficulty may only stem from cyber-on-cyber

deterrence. It is entirely plausible that a state could successfully deter an unwanted action in cyberspace through linking it to a conventional response, provided the threat of the latter was credible.

The literature has identified several factors that make deterrence in cyberspace difficult. First, problems of attribution could undermine deterrence through obscuring the source of the deterrent threat, absent some coupling mechanism. Second, deterrence through punishment in cyberspace is nearly impossible given the current state of the field, whereby an overwhelming campaign to deliver devastating pain and suffering on an enemy population is not yet feasible. However, this may change as technology changes. Third, deterrence through denial is difficult due to the perceived ease of offensive operations and the fact that there are always vulnerabilities an attacker can exploit. Fourth, the multiplicity of actors in cyberspace complicate deterrence because it may not be clear who needs to be deterred and difficult to identify what they value in order to affect their cost-benefit calculus. There is a plethora of actors actively engaged in this domain, which run the gamut from nation states to criminal organizations, individual hackers, patriotic groups, private corporations, terrorist organizations, and others.

While the academic literature has begun to explore the conditions under which deterrence can be achieved in cyberspace, few scholars have tackled the issue of compellence in cyberspace. Many of the same problems associated with deterrence in cyberspace also apply to compellence. It is important to note, however, that reassurance plays a particularly important role in compellence, especially in the context of the limited application of force. If the target does not believe that compliance will result in the cessation of punishment, there is little incentive to comply. Reassuring a target in cyberspace is difficult due to problems of command and control—it may be difficult to put the genie back in the bottle once a capability is unleashed. Compellent threats also engage the target's reputation, making face-saving mechanisms more important. It is unclear how this can be done effectively in cyberspace.

Further unpacking the nature of deterrence and compellence, which are central the conduct of strategy, is imperative for effective use of cyber power. Questions on this front include:

- Which insights from the conventional and nuclear deterrence literatures are applicable to the study of cyber deterrence, and which fall short? What does this suggest about the nature of deterrence in cyberspace?
- In the context of cyber deterrence, what is the relationship between the cyber domain and other domains, both in terms of the behavior to be deterred as well as the means of deterrence?
- Despite the structural challenges to cyber deterrence, why have significant strategic vulnerabilities and the widespread availability of attack tools not resulted in large-scale attacks? Is a tacit deterrent holding that we don't understand?
- What is the logic of coercion in cyberspace?
- Is it possible to deter nonstate actors in cyberspace?
- How does one conduct a cost-benefit analysis of cyber punishment?

Attribution and Multiple Actors

States take measures to avoid attribution in conventional domains because they value plausible deniability. Typically, states do so because they want to either hide their activities from domestic audiences or allies, or they want to avoid conflict escalation or retaliation by an adversary. Governments may also want to obscure their association with certain activities if they violate international laws or norms, or would otherwise undermine the states' reputation. States can obscure their footprints by operating through covert or clandestine means, which often includes working with proxy groups and other intermediaries to distance the government from operations on the ground. From a strategic perspective, there may be tradeoffs between plausible deniability and effectiveness, and governments may encounter difficulties controlling the behavior of the proxies on their payrolls.

Issues associated with attribution in cyberspace differ from conventional domains, primarily due to the greater difficulties associated with the former. Put simply, governments have to go to great lengths in conventional domains to hide their activities due to the relative ease of attribution. Absent significant efforts to conceal the origins of an attack, targets in conventional domains can easily identify its source. Conversely, attribution presents far greater hurdles in cyberspace, despite the fact that governments are improving their attribution capabilities. Attribution is hard for a number of reasons. From a technical perspective, actors can spoof the source of an attack, and even if a government can ascertain the location of an attack with a high degree of confidence, the opacity of command and control means that there could be little certainty about who was sitting at the keyboard at the time of the attack. Furthermore, a number of attribution techniques rely on pattern analysis, to include target sets, timing of the attack, and methodology, as well as unique signatures embedded in the

code. Attribution can also be corroborated with some degree of confidence by analyzing contextual political cues, such as an ongoing conventional operation that occurs simultaneous to a cyberattack. However, a savvy operator may still spoof these attibution technqiues. The highest degree of attribution can be attained if a target has preexisting access to the state issuing the attack and witnesses an attack occurring in real time; however, there may be incentives not to reveal this information because doing so could compromise the access vector.

Complicating problems of attribution is the multiplicity of actors operating in cyberspace, as mentioned above. Governments could employ many of these actors as proxy groups when the former lack the capabilities to engage in certain kinds of cyberattacks or seek to conduct plausibly deniable attacks. Some of the same problems associated with proxy warfare in the traditional sense also manifest in cyberspace.

In recent events, political leaders have demonstrated a greater willingness to attribute cyberattacks to governments as well as nonstate groups. Furthermore, the private sector has developed more sophisticated capabilities to attribute attacks against infrastructure, systems, and intellectual property, exploiting their sensors within customer networks to which the government does not have ready access. Moreover, policymakers have become more inclined to publicly substantiate attributional claims made by private cybersecurity corporations. Altogether, this suggests that we are likely to observe public attributions occurring with greater frequency in the future. However, this could create unanticipated consequences. To wit, increased public attribution may push governments to rely more on proxy groups, because these relationship support more ambiguous command and control to enable plausible deniability and allow states to surmount the greater ease of technical attribution. Some questions that might expand our understanding of attribution dynamics include:

- What are the strategic implications of attribution problems? What aspect of the attribution problem poses greater difficulty for governments—technical barrier to attribution or political ones?
- To what extent does attribution impact the range of responses available to governments?
- Can the attribution problem be quantified?
- What dangers do states employing cyber proxies pose? What policy prescriptions follow from this?

Strategic Stability in Cyberspace

During the Cold War, the conditions under which strategic stability could be achieved were of paramount concern to academics and policymakers, as the superpowers sought to avoid cataclysmic nuclear war. Nuclear deterrence, as described above, created stability at the systemic level, because the threat of mutually assured destruction, which rested on secure second strike capabilities, negated a first strike advantage in a nuclear exchange. However, the stability of mutual deterrence also led to the stability-instability paradox. This meant that, while the nuclear-armed superpowers were deterred from a strategic nuclear exchange, this very stability at the systemic level enabled them to engage in low-level conflict (precisely because nuclear deterrence took nuclear war and attacks against the homeland off the table). Paradoxically, however, this low-level conflict could create instability and threaten to spiral into a nuclear engagement—the very thing that was supposed to be unthinkable.

As demonstrated above, mutual deterrence is problematic in cyberspace. Therefore, the domain is more likely to suffer from problems of cyber instability. These challenges are exacerbated by the fact that there are few norms governing acceptable behavior in cyberspace, contributing to additional problems of misperception and crisis instability. While the logic of the stability-instability paradox is not perfectly applicable to cyberspace because the stability of nuclear deterrence is not present in this domain, there are nevertheless some lessons we can derive from the idea that when certain courses of action are defined as outside of the realm of the plausible, that may enable risk-taking behavior that contributes to instability. Put differently, it is widely accepted by policymakers and scholars that a cyber Armageddon is unlikely to occur. This may unintentionally enable more risk-taking behavior by governments in cyberspace if they believe they can get away with cyberattacks, due to problems of attribution, revisionist aspirations, or ambiguous norms governing acceptable responses and proportionality.

Arms control regimes have also contributed to systemic stability through changing the incentive structures states have for going to war. In practice, this involves mechanisms for transparency and information sharing, crisis prevention, arms limitations (both quality and quantity), and shaping policies for arms employed during conflict. Once an arms control agreement has been reached, the key aspects that contribute to its effectiveness include monitoring, compliance, and enforcement. Monitoring for compliance in cyberspace is nearly impossible because no government would be willing to grant access to sensitive networks. Moreover, the ease of defection makes whatever access may be granted to a monitoring authority irrelevant. Historically, when sensitive accesses were required for compliance, states have relied on national

technical means, such as overhead collections, to monitor for compliance. However, the equivalent of national technical means in cyberspace would require conducting espionage against these sensitive networks, which may further add to instability if the intent of these operations is misinterpreted. Finally, attribution problems complicate enforcement of arms control regimes.

A final factor in the international relations literature concerning stability is the distribution of power in the system, with power defined as military capabilities. While most scholars would agree that the international system is currently unipolar, the cyber domain is the only area where the unipole faces near-peer competitors. In other words, while the international system is unipolar, the cyber system is multipolar. This has interesting implications for stability. Debates surrounding the stability of multipolar systems remain unsettled in the realist paradigm. Related to this are the stability implications associated with the offense-defense balance, the cult of the offensive, and prevailing doctrines. Multipolarity in cyberspace is likely to be more destabilizing than in the conventional realm due to the difficulties described above concerning how we measure cyber capabilities are measured—there are no measures of relative strength. Moreover, states may be willing to act in revisionist ways due to attributional issues, believe they can overcome asymmetries of power that exist in the physical domains of warfare. Regarding these issues, future research questions include:

- What are the conditions under which the cyber system is stable versus unstable?
- How should we define stability in the cyber domain?
- What does cyber arms control look like? Is it achievable?
- How can governments best build redundancy and resiliency to ensure survivability? What are the priorities of survivability?

Conclusion

The field of cybersecurity studies is wide open for scholars to make meaningful contributions that directly impact national security policy. In many ways, this resembles the early years of the Cold War, when the uncertainty surrounding the implications of nuclear weapons and bipolarity created an opportunity for academics to play a significant role in strategic thought and practice. During the Cold War, it took the Cuban Missile Crisis for governments to truly recognize the gravity of the issues at stake. Hopefully, it will not take a comparable crisis in cyberspace to prompt academics and policymakers to develop a comprehensive strategy for the domain. •

IMPORTANT WORKS

F. D. Kramer, Starr, S. H., and L.K. Wentz Eds. Cyberpower and National Security. Potomac Books, Inc., 2009.

Greg Rattray, Strategic Warfare in Cyberspace. MIT Press, 2001.

Joseph S. Nye, "Cyber Power." Essay form the Belfer Center for Science and International Affairs, Harvard Kennedy School May 2010.

Thomas Rid and Peter McBurney, "Cyber Weapons." The RUSI Journal 157 (1): 6-13, 2012.

Martin C. Libicki, Conquest in Cyberspace, Cambridge: Cambridge University Press, 2007.

Brandon Valeriano and Ryan C. Maness. Cyber War versus Cyber Realities: Cyber Conflict in the International System (New York: Oxford University Press), 2015.

Adam Segal, Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, Public Affairs, 2016.

Martin C. Libicki, Cyberdeterrence and Cyberwar. Rand Corporation, 2009.

Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. Vol. 58. 2010.

Joseph Nye, "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly. Winter 2011.

Richard L. Kugler, "Deterrence of Cyber Attacks." In Cyberpower and National Security, Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 2009.

Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," (Working paper)

Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risk in Using Cyber Proxies?," Orbis, Summer 2016.

Tim Maurer and Kenneth Geers. "Cyber Proxies and the Crisis in Ukraine," NATO CCD COE Publications (2015).

Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," Air University, 2012.

Martha Finnemore, "Cultivating International Cyber Norms." America's Cyber Future: Security and Prosperity in the Information Age 2 (2011).

IMPORTANT WORKS

Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security." Belfer Center Discussion Paper 2011-11, September 2011.

Brian Mazanec, The Evolution of Cyberwar: International Norms for Emerging Technology Weapons. (Lincoln: University of Nebraska Press), 2015.

Emilio Iasiello, "Hacking Back: Not the Right Solution." Parameters 44.3 2014: 105.

Ruperto P., Majuca and Jay P. Kesan, "Hacking Back: Optimal Use of Self-Defense in Cyberspace." Chicago-Kent Law Review 84.3 (2010): 08-20.

James A. Lewis, "Sovereignty and the Role of Government in Cyberspace." Brown J. World Aff. 16 (2009): 55

Stephen K. Gourley, "Cyber Sovereignty," Conflict and Cooperation in Cyberspace: The Challenge to National Security (2013): 277.

Chris C. Demchak, and Peter Dombrowski. "Rise of a Cybered Westphalian age," Air University Maxwell Air Force Base, Strategic Studies Quarterly, 2011.

Herbert Lin, "Arms Control in Cyberspace: Challenges and Opportunities." World Politics Review, March 6, 2012.

Robert K. Knake, Internet Governance in an Age of Cyber Insecurity (No. 56), 2014.

Laura DeNardis, The global war for Internet governance. Yale University Press, 2014.

Milton L. Mueller, Networks and States: The Global Politics of Internet Governance. MIT Press, 2010.

Global Commission on Internet Governance Paper Series. Centre for International Governance Innovation (CIGI), https://www.cigionline.org/series/global-commission-internet-governance-paper-series.

Conference on Internet Governance and Cyber Security background papers. Columbia University School of International and Public Affairs. https://sipa.columbia.edu/experience-sipa/cross-cutting-initiatives/cyber-security/background-papers.

CYBER CONFLICT HISTORY

Columbia University	**Rapporteur: Karl Grindal** **Moderator: Jason Healey**
June 16, 2016	

Introduction

Cyber conflict history is an essential starting point for addressing a number of the critical policy and discipline-oriented questions proposed throughout the workshop. Case studies and historical datasets provide academic fuel to develop quantitative methodologies and testable hypotheses. The identification of canonical works that shape the field can bridge generational and subject area divides and provide a baseline for core knowledge shared by the community. Further, oral histories provide context from the complex web of interconnected perspectives, explaining the reasoning behind individuals' actions. While broad in scope, this historical approach is about more than just presenting facts, but rather about finding patterns and establishing meaning in our shared history.

Specific to cyber, there are a number of complicating factors in documenting cyber history. These include not only the secrecy surrounding government organizations and their capabilities, but also the anonymity of attackers. Further, the recent and rapid growth in the field means the subject has yet to receive adequate attention from professional historians. Consequently, the field has begun to structure its own history, with publications like *A Fierce Domain* (Healey 2013) leading the way, with a number of popular histories coming out in just the past year (e.g., Kaplan 2016, Malconsin 2016, and Ridd 2016). As this history gets written, the field must deal with a number of meta-level concerns including: defining cyber's origins, mapping the development of the field, and identifying historical eras. Organizational, operational, and nonstate histories will help to further subdivide this analysis. Outside of public reporting, the principal source of new historical information may flow from participants themselves in the form of oral histories.

Topic:	**Questions:**	**Gaps:**
Origins of Cyber Domain	How did the institutions and norms developed around cryptography and early computing shape cyber conflict? How should we understand the convergence of IA, SIGINT, and CNA?	Evolution of IW and EW capabilities into the cyber conflict field of today. Most research is still US-centric. Focus is on government at the expense of the private sector.

One of the first questions posed to participants was how to define the technological era being circumscribed. While there is disagreement over the unit of analysis based on how cyber is defined, there are established predecessors to the networked society created by the rise of the Internet. Participants did not resolve whether cyber's antecedents should include a more expansive understanding of networked information that incorporates telegraph and radio communications or be more narrowly defined as beginning with either the IP protocol or the origin of a self-identified field of study.

Early Predecessors

The discussion of this expansive definition of cyber incorporated both historical sources and contemporary research. Many participants had read works by Herbert Yardley, a leading American cryptanalyst during the early twentieth century. While Yardley's personal writings are heavily biased based on his personal experience, the historian David Kahn's biography *The Reader of Gentleman's Mail* was proposed as a preferable canonical work. However, Yardley's book describing his work for Chiang Kai-shek's Nationalists in *The Chinese Black Chamber* was discussed favorably.

Several anecdotes were mentioned as the discussion delved into nations' use of the global telegraph system for strategic purposes. These included the US decision to cut telegraph wires to Cuba during the Spanish—American War in 1898, establishing an acceptable norm in what had previously been an ambiguous legal space. These actions were repeated during WWI when the British cut Germany's telegraph wires. One of the consequences of this move was Germany's use of British infrastructure when sending the Zimmerman telegraph to Mexico. The interception and publication of this telegraph shaped history by bringing the United States into the war and helped to tip the balance in favor of the allies.

Several of these historical incidents have been explored in greater depth in Emily Goldman and John Arquilla's "Cyber Analogies." A more detailed survey of this telegraph history was identified in Hendrick (1991), with a specific description of imperial cable communications network and strategy of the United Kingdom in Kennedy (1971), and telegraph network history in Iran in Rubin (2004, 1998, 2001). The British assertion of communications dominance during WWI extended to radio. Lamber (2012) was cited as an exploration of the impact on the Royal Navy. Brief mention was made of the history of computing and cryptography. Histories of Bletchley Park and the decoding of the Enigma Cipher have been explored in significant detail in foundational works, including Kahn (1996).

While WWII was discussed in the context of technical spoofing and disruption, the discussion then shifted to the more challenging historical documentation of cryptography and communications during the Cold War. The development of cybernetics during the Cold War inspired both the name of the discipline and much of the theoretical tradition behind cyber studies. Participants saw Ridd (2016) as an approachable survey of this material, while Norbert Wieners' Cybernetrics was the foundational publication that launched the discipline. David Hoffman's *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* was identified as a revealing book on the command and control (C2) issues that plagued the era. Specific to US intelligence, the group highlighted Tom Johnson's history of the NSA four-volume series (*American Cryptology during the Cold War, 1945-1989*) as a go-to primary source. As the NSA historian with more direct access to agency records, Johnson's work is seen as superior to that of James Bamford, whose 1982 book *The Puzzle Place* provided the public with its first exposure to the NSA's critical but secretive role in US history.

Two additional questions that came out of our discussion were: 1) how did the different disciplines of information assurance, computing, SIGINT, counterintelligence, and computer network attack combine? and 2) how did the US experience differ from that of the Chinese and Russians?

Topic:	**Questions:**	**Gaps:**
Development of the Field	Which early works helped to develop the field of cyber conflict studies? Why were many foundational documents developed outside academia?	The impact of conferences, list serves, and magazines in shaping the field. The role of industry associations and user groups. How did early researchers shape and inform each other's perspectives of the field?

The discussion of the state of the field extended our analysis from a substantive focus on computer and network security to early government reports, academic scholarship, and journalistic discussion on the implications of an increasingly networked and vulnerable world.

The group acknowledged the relevance of historical lessons and their ready application to the present, reflecting on a quote by Roger Shell "Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought" back in 1979. Other prescient publications identified by the group, included the following:

- **Willis Ware - Ware Report**
- **Donn Parker 1976 "Crime by Computer"**
- **Bell Podier Report - from the air force, classification system**
- **Vint Cert - classified Discussion with NSA, National Computer Security Center in 1984.**
- **Defense Science Board (DSB) Reports- '95 and '96.**
- ***Information Terrorism: Can You Trust Your Toaster* by Matt Devost, Brian Houghton, and Neal Pollard back in 1996.**
- **Bruce Schneier's "Secrets and Lies: Digital Security in a Networked World" published in 2000.**

The group shared the understanding that the highly technical, secretive, and multidisciplinary aspects of cybersecurity had presented a challenge to traditional scholarship. Consequently, security practitioners developed their own outlets for reflection that included conferences, periodicals, and listservs. Phil Lappsley's book *Exploding the Phone: Declassified Interviews with Phreakers* was mentioned as a publication that gave voice to early hackers.

Early inspirational authors who tapped into the potential within the field included works Winn Shwartau and Alvin Toffler, while Dorothy Denning provided an early scholarly approach in her analysis of the field. The group also sought to give credit to David Ronfield, who in 1992 was writing with John Arquilla, the "Dark Prince" at RAND.

Topic:	**Question:**	**Gaps:**
Eras in Cyber Conflict History	How can we divide cyber conflict history into eras? What incidents or moments serve as transition points between these eras? What has been the changing balance between military operations and intelligence as a matter of doctrine, organization, and practice?	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?

Having raised questions on the formation of the field, its evolution represents a natural secondary question. Attempting to look at the field with a macro-level of analysis, it is useful to use the historical terms of "era" to circumscribe those periods of time when cyberspace or the cyber policy environment was significantly transformed.

These periods of time are often demarcated by unique attributes. The field currently lacks a common terminology for eras within cyber conflict history; however, some effort was made to define these eras in Healey (2013). In *A Fierce Domain*, the designation of the "realization" stage in the 1980s, "takeoff" starting in 1998, and "militarization" starting in 2003 provides an initial structure that identifies particular energy around the turn of the century. A broader discussion of eras in the evolution of intelligence is found in Warner (2014).

The group identified several incidents that might signal shifts in eras including Morris Worm in 1998, Blaster in 2003, and the recognition of Chinese espionage starting around 2005 (attribution based on the location of C&C nodes and the list of victims). The field accelerated further around 2009, when a pivot began as the number of case studies grew. These new case studies focused on incidents attributed to Russia or China, including the Project Grey Goose Phase II report, the US-CCU Special Report Overview of the Cyber Campaign Against Georgia in August of 2008, as well as GhostNet and Shadows in the Cloud. While the role of these case studies, referred to at the time as "wake up calls," may illuminate transitions in cyber conflict history eras, the discussion highlighted a concern among participants that the incremental availability of public case studies may affect the capacity to draw conclusions if they are not reflective of non-public incidents.

Topic:	**Questions:**	**Gaps:**
Organizational History	How have legislation, rules, doctrines, and norms evolved to address cyber threats? How did major cyber incidents impact organizational policies or structures? Were doctrinal and organizational developments abroad secondary or primary factors for domestic organizational change? How have organizations adopted and incorporated offensive cyber capabilities?	Weighted towards institutions that either defended or threatened the United States. The impact and evolution of non-governmental organizations is underexplored.

In an effort to deconstruct the history of the Joint Task Force for Computer Network Defense, Healey (2013) focuses on shifts in the balance of offensive versus defensive missions as well as questions of normality. When defined as a domain, cyber often is

seen as needing different kinds of people, much like special operations. When normalized, cyber gets integrated back into operations. The tensions between these competing missions help to clarify evolutions in the organizational history and origins of Cyber Command.

Another organizational history question is the competing aspects of centralization and decentralization. The establishment of the Department of Homeland Security (DHS), for example, provides a centralizing moment in combing the National Infrastructure Protection Center (NIPC) and the Critical Infrastructure Assurance Office (CIAO) within a shared organization.

Two relevant works were discussed as focusing on this organization history: Michael Hayden's memoir *Playing to the Edge: American Intelligence in the Age of Terror* as well as the chapter "The U.S. Cyber Command's Road to Full Operational Capability" by Michael Warner in *Stand Up and Fight! The Creation of U.S. Security Organizations, 1942-2005*, released by the Army War College Press in 2015.

In contrast with the American experience, the discussion highlighted the importance of the concepts of electronic warfare and information warfare to the development of cyber conflict capabilities and doctrine in Russian and Chinese history. This led to recognition that the Chinese have a twenty-year lead on the United States in EW and cyber integration with respect to doctrine. Their intra-People's Liberation Army (PLA) organizational debate on the structure of cybersecurity or electronic warfare was led by Dai Qingmin, who argued that EW should be the contextual framework, and Xu Xiaoyan, who suggested that cyber should be the lead. Dai Qingmin is seen as having won the argument. With respect to Russian history, the merits of Tim Thomas were discussed for his analysis. While recommended, participants suggested that his work mapped closely to what was translated by the Director of National Intelligence's Open Source Center (OSC), but may have missed information published elsewhere.

The group did wish to see more work done on the history of military exercises as a demonstration of capability and coordination. CCSA had pursued developing a "History of Training" and a "History of Exercises" during work on *A Fierce Domain*; however, nothing has yet been published.

Topic:	Questions:	Gaps:
Operational History	How did operators identify, protect, detect, respond, and recover from major cyber incidents? Are there lessons from these operational incidents that can inform current cyber defenders or policymakers?	Comprehensive case studies or timelines for all but the most significant incidents. Analysis of incidents using historical datasets is still limited to a few scholars.

The discussion of the operational history focused on state actors' use of offensive cyber weapons and the consequent response and recovery of their targets. While the discussants acknowledged the challenges in compiling a comprehensive timeline of these incidents, the increasing willingness of private actors to expose state-sponsored activity has dramatically expanded access to case studies. This relatively novel trend has changed some operational dynamics by placing increasing importance on how offensive actors respond to the disclosure of their attacks. One participant described this as an iterative game of exposure.

Members expressed frustration that analysis has continued to focus on a select few case studies from earlier in cyber history and that the field has yet to incorporate rich contemporary case studies into its analysis. One example of a richer case studies that is infrequently mentioned in the literature is the hacking of elections in Latin America by Andrés Sepúlveda who was employed political sabotage in support of campaigns in Mexico, Venezuela, and Colombian between 2008 and 2012. Another sources of case studies is the technical literature on the takedowns of botnets. An understanding of the hybrid use of botnets helps to connect the story of cybercrime and cyber conflict in Russia in particular. However, Western actors like GCHQ were not seen as irreproachable having enabled botnets in Belgacom's network. Some of the well-documented botnet takedown discussed included:

Conficker[44] – 2008

ZeuS – 2009

Gameover ZeuS – 2014

44 Worm: The First Digital World War by Mark Bowden

The Security Service of Ukraine (SBU) was discussed as having made a strong Conficker attribution case. However, conflict in the region means the team that was involved are no longer accessible and none of the material was translated.

Other case studies, both real and imagined that were discussed included:

- **Iraqi printer hoax - 1991**
- **Turkish pipeline missreporting – 2008**
- **Symantec's Dragon fly / Kaspersky Energetic Bear - 2010**
- **Careto/Mask APT - 2014 (Kaspersky exposed a major counter terrorism operation and did so essentially for marketing purposes.)**

The group agreed that operational history should not be confined merely to building timelines and case studies, as there are other critical questions facing the field. These include the following:

1. **How have conflicts been fought?**
2. **What are the inflection points?**
3. **Which dynamics have been stable? Which have changed??**
4. **Is the nature of cyber conflict more about history or opportunity?**

Topic:	**Question:**	**Gaps:**
History of Nonstate Actors	How have nonstate actors' capabilities evolved? How have nonstate actors shaped the domain? Do offensive actions by nonstate actors meet their objectives?	Focus on contemporary case studies at the expense of historical activity. Lack of understanding of the sharing of resources, tools, and techniques across groups and between individuals.

As the conversation shifted from state-based organizations and operations to the activity of nonstates, the larger question arose of whether cyber has operated in a post-structuralist or post-Westphalian reality. The plurality of actors in the cyber environment led to a brief definitional conversation on the role of nonstates in IR

theory. The group was divided on whether the terminology of non-governmental organizations on nonstate actors presented a more appropriate term for the discussion, and failed to find consensus. Despite terminology disputes, there was broad consensus about the significance of both threat actors and private sector actors in the cyber domain.

Complicating this conversation further is the question of how to categorize patriotic hacking, which started up around 1997. Should patriotic hackers be classified as state actors? Also discussed was the number of participants in these groups that either fall away or become integrated into the government or security industry.

Participants also converged around the importance of high-trust, deeply vetted sharing networks. Organizations including ISPs, vendors, NSP-SEC, the Internet Security Operations and Intelligence (ISOI) workshop, the Anti-Phishing Working Group, and FS-ISAC were briefly discussed. The adversarial relationship between tech companies, government, and intelligence complicates the relationship between many private sector technology companies. Participants shared several anecdotes citing this conflict between the US government and Microsoft dating back decades, including US government sources identifying Microsoft as a greater security threat than China. Microsoft, for its part, opened an office in China starting sometime near the early aughts without disclosing the relevant details to the US government. The increasing assertiveness of the private sector has led companies to assume traditional governance roles, with Microsoft dropping proposed cyber norms over the summer of 2016. Marc Sachs at Verizon was paraphrased by a participant as saying, “we’re creating cyberspace, we can bend it if we need to.” Despite the significant role of private sector actors, cybersecurity is often a secondary priority for these organizations. Verizon’s decision to let botnet traffic move on Autonomous System Numbers AS701 and AS702 based on the risk of indemnification and the lack of financial gain was also referenced. With respect to offensive cyber actors, the group discussed the legitimation of offensive teams like Hacking Team and the sale of these capabilities dating back to the 1990s.

CYBER CONFLICT HISTORY

Topic:	Question:	Gaps:
Narratives of Practitioners	What was the lived experience of cyber professionals? How have different disciplines interpreted the same historical moments? How might historical perspectives inform current debates about the structure and nature of cyber institutions?	The field lacks professional oral histories. Rarer still are moments when offensive and defensive actors experienced the same incident.

The lack of oral histories in the field represents an obvious place for a formal documentation of cyber conflict history. Current projects worth mention include Jeffrey Yost and Thomas Misa at the University of Minnesota's Charles Babbage Institute, who have developed an oral history of Symantec and hosted a conference on cybersecurity history in 2014. Current oral history projects to date seem to have been regionally focused on Northern California. Potentially relevant work includes research out of the Bankcroft Library at Berkeley, which hosts the Regional Oral History Project, as well as *A History of Silicon Valley* (Rao and Scaruffi 2011).

The discussion briefly acknowledged the challenges of getting some leading actors to participate in documenting this history. The secrecy of the subject remains an obstacle to getting significant actors on the record, like Jim Gosler of the Defense Science Board. The group cited publicly available court documents as an insufficiently explored potential source; however, accessing many of these documents might require physically visiting local courthouses. •

IMPORTANT WORKS

Topic: Origins of Cyber Domain

Bamford, James. Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. 1st Anchor Books ed. New York: Anchor Books, 2002.

The Puzzle Palace: A Report on America's Most Secret Agency. Harmondsworth, Middlesex ; New York, NY: Penguin Books, 1983.

Kahn, David. The Codebreakers: The Story of Secret Writing. Rev. ed. New York: Scribner, 1996.

M. Rubin, "The Indo-European Telegraph Department." Encyclopaedia Iranica. Vol. 13, Fasc. 1.

New York: Center for Iranian Studies, 2004.

M. Rubin, "The Telegraph, Espionage, and Cryptology in 19th Century Iran." Cryptologia.

January 2001. pp. 18 - 36.

M. Rubin, "The Telegraph and Frontier Politics: Modernization and the Demarcation of Iran's

Borders." Comparative Studies of South Asia, the Middle East, and Africa. Fall 1998. pp. 59 - 72.

Yardley, Herbert O. The American Black Chamber. Bluejacket Books. Annapolis, Md: Naval Institute Press, 2004.

Topic: Development of the Field

Arquilla, John, and David Ronfeldt. Networks and Netwars: The Future of Terror, Crime, and Militancy. 1st ed. Rand Corporation, 2001.

Denning, Dorothy E. Information Warfare and Security. 1st ed. Addison-Wesley Professional, 1998.

Rattray, Gregory J. Strategic Warfare in Cyberspace. Boston, MA: MIT Press, 2001.

Schwartau, Winn. Information Warfare: Second Edition. 2nd ed. Thunder's Mouth Press, 1996.

Toffler, Alvin, and Heidi Toffler. War and Anti-War: Making Sense of Today's Global Chaos. Grand Central Publishing, 1995.

IMPORTANT WORKS

Topic: Eras in Cyber Conflict History

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

Kaplan, Fred M. Dark Territory: The Secret History of Cyber War. First Simon & Schuster hardcover edition. New York: Simon & Schuster, 2016.

Warner, Michael. "Cybersecurity: A Pre-History." Intelligence and National Security 27, no. 5 (October 2012): 781–99. doi:10.1080/02684527.2012.708530.

Topic: Organizational History

DeNardis, Laura. "The Internet Design Tension between Surveillance and Security." IEEE Annals of the History of Computing 37, no. 2 (April 2015): 72–83. doi:10.1109/MAHC.2015.29.

Joseph Ruffini. "609 IWS Chronological History." Department of the Air Force, June 30, 1999. http://securitycritics.org/wp-content/uploads/2006/03/hist-609.pdf.

"JTF-CND / JTF-CNO / JTF-GNO -- A Legacy of Excellence," n.d.

Lipner, Steven B. "The Birth and Death of the Orange Book." IEEE Annals of the History of Computing 37, no. 2 (April 2015): 19–31. doi:10.1109/MAHC.2015.27.

Yost, Jeffrey R. "The Origin and Early History of the Computer Security Software Products Industry." IEEE Annals of the History of Computing 37, no. 2 (April 2015): 46–58. doi:10.1109/MAHC.2015.21.

Topic: Operational History

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Proceedings of the 7th European Conference on Information Warfare, 2008, 163.

Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal, January 6, 2011.

Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. First Edition. New York: Crown Publishers, 2014.

IMPORTANT WORKS

Topic: History of Nonstate Actors

Dreyfus, Suelette, and Julian Assange. Underground. 1. publ. Edinburgh: Canongate, 2012.

Hafner, Katie, and John Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster, 1995.

Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam, 1993.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Pocket Books, 1990.

Coleman, E. Gabriella. Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous, 2015.

Topic: Narratives of Practitioners

Cox, Samuel, Matt Devost, Sean Kanuck, and Jason Healey. Lessons from Our Cyber Past: History of Cyber Intelligence. Atlantic Council, 2012. http://www.atlanticcouncil.org/events/past-events/lessons-from-our-cyber-past-history-of-cyber-intelligence.

Lieutenant General John H. "Soup" Campbell, USAF (Ret.), Major General James D. Bryan, USA (Ret.), and Colonel Walter "Dusty" Rhoads, USAF (Ret.). Transcript: Lessons from Our Cyber Past - The First Military Cyber Units, March 5, 2012. http://www.atlanticcouncil.org/news/transcripts/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units.

Landwehr, Carl E. "History of US Government Investments in Cybersecurity Research: A Personal Perspective," 14–20. IEEE, 2010. doi:10.1109/SP.2010.41.

Painter, Christopher, Steve Chabinsky, and Shawn Henry. Transcript: Lessons from Our Cyber Past - The First Cyber Cops, May 6, 2012. http://www.atlanticcouncil.org/news/transcripts/lessons-from-our-cyber-past-the-first-cyber-cops-transcript-05-16-12.

MORE SOURCES: POTENTIALLY OVERLAPPING

Arquilla, John, and David Ronfeldt. Networks and Netwars: The Future of Terror, Crime, and Militancy. 1st ed. Rand Corporation, 2001.

Bamford, James. Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. 1st Anchor Books ed. New York: Anchor Books, 2002.

The Puzzle Palace: A Report on America's Most Secret Agency. Harmondsworth, Middlesex ; New York, NY: Penguin Books, 1983.

Coleman, E. Gabriella. Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous, 2015.

Cox, Samuel, Matt Devost, Sean Kanuck, and Jason Healey. Lessons from Our Cyber Past: History of Cyber Intelligence. Atlantic Council, 2012. http://www.atlanticcouncil.org/events/past-events/lessons-from-our-cyber-past-history-of-cyber-intelligence.

DeNardis, Laura. "The Internet Design Tension between Surveillance and Security." IEEE Annals of the History of Computing 37, no. 2 (April 2015): 72–83. doi:10.1109/MAHC.2015.29.

Denning, Dorothy. Information Warfare and Security. Addison-Wesley Professional, 1998.

Dreyfus, Suelette, and Julian Assange. Underground. 1. publ. Edinburgh: Canongate, 2012.

Evron, Gadi. "Battling Botnets and Online Mobs." Georgetown Journal of International Affairs 9, no. 1 (February 2008): 121.

Franklin, Derek. "Information Warfare: Issues Associated with the Defense of DOD Computers and Computer Networks." USMC Command and Staff College, 2002. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA404740.

Hafner, Katie, and John Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster, 1995.

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

Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal, January 6, 2011.

Joseph Ruffini. "609 IWS Chronological History." Department of the Air Force, June 30, 1999. http://securitycritics.org/wp-content/uploads/2006/03/hist-609.pdf.

"JTF-CND / JTF-CNO / JTF-GNO -- A Legacy of Excellence," n.d.

Kahn, David. The Codebreakers: The Story of Secret Writing. Rev. ed. New York: Scribner, 1996.

Kaplan, Fred M. Dark Territory: The Secret History of Cyber War. First Simon & Schuster hardcover edition. New York: Simon & Schuster, 2016.

Landwehr, Carl E. "History of US Government Investments in Cybersecurity Research: A Personal Perspective," 14–20. IEEE, 2010. doi:10.1109/SP.2010.41.

Libicki, Martin. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND, 2009.

Defending Cyberspace and Other Metaphors. Washington, DC, 1997.

Lieutenant Colonel Roger Schell. "Computer Security: The Achilles' Heel of the Electronic Air Force?" Air University Review 30, no. 2 (January 1979): 16–33.

Lieutenant General John H. "Soup" Campbell, USAF (Ret.), Major General James D. Bryan, USA (Ret.), and Colonel Walter "Dusty" Rhoads, USAF (Ret.). Transcript: Lessons from Our Cyber Past - The First Military Cyber Units, March 5, 2012. http://www.atlanticcouncil.org/news/transcripts/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units.

Lipner, Steven B. "The Birth and Death of the Orange Book." IEEE Annals of the History of Computing 37, no. 2 (April 2015): 19–31. doi:10.1109/MAHC.2015.27.

Malone, Eloise F., and Michael J. Malone. "The 'wicked Problem' of Cybersecurity Policy: Analysis of United States and Canadian Policy Response." Canadian Foreign Policy Journal 19, no. 2 (June 1, 2013): 158–77. doi:10.1080/11926422.2013.805152.

Mitnick, Kevin D, and William L Simon. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. New York: Little, Brown & Co., 2012.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Proceedings of the 7th European Conference on Information Warfare, 2008, 163.

Painter, Christopher, Steve Chabinsky, and Shawn Henry. Transcript: Lessons from Our Cyber Past - The First Cyber Cops, May 6, 2012. http://www.atlanticcouncil.org/news/transcripts/lessons-from-our-cyber-past-the-first-cyber-cops-transcript-05-16-12.

Rattray, Gregory J. Strategic Warfare in Cyberspace. Boston, MA: MIT Press, 2001.

Schwartau, Winn. Information Warfare. New York, NY: Thunder's Mouth Press, 1996.

Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam, 1993.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Pocket Books, 1990.

Toffler, Alvin, and Heidi Toffler. War and Anti-War: Making Sense of Today's Global Chaos. Grand Central Publishing, 1995.

W. H. Ware. "Future Computer Technology and Its Impact." Santa Monica, CA: RAND Corporation, November 1965. http://www.rand.org/content/dam/rand/pubs/papers/2008/P3279.pdf.

Warner, Michael. "Cybersecurity: A Pre-History." Intelligence and National Security 27, no. 5 (October 2012): 781–99. doi:10.1080/02684527.2012.708530.

Yardley, Herbert O. The American Black Chamber. Bluejacket Books. Annapolis, Md: Naval Institute Press, 2004.

Yost, Jeffrey R. "The Origin and Early History of the Computer Security Software Products Industry." IEEE Annals of the History of Computing 37, no. 2 (April 2015): 46–58. doi:10.1109/MAHC.2015.21.

Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. First Edition. New York: Crown Publishers, 2014.

LEGAL AND ETHICAL ISSUES

Columbia University	**Moderator: Harvey Rishikof** **Rapporteur: Douglas Cantwell[45]**
June 17, 2016	

45 Lieutenant Junior Grade, Judge Advocate General's Corps, US Navy. At the time of the conference, Douglas Cantwell was serving as the inaugural Detlev F. Vagts fellow at the American Society of International Law. The author participated in the conference solely in his personal capacity. The views expressed in this chapter do not necessarily represent the views of the Department of the Navy, the Department of Defense, or the United States. Likewise, the views expressed herein do not necessarily represent the views of the American Society of International Law.

Introduction

Operations in the cyber domain act within national and international legal regimes; the Internet is not a wild west. While legal ambiguity and challenges in enforcement remain, lawyers have slowly been developing precedent and legal treaties to bind countries to certain norms. Understanding these rules, their formation, and area where concensus has yet to form can help us to understand organizational and state behavior. This discussion provided an opportunity to reflect on how the law of cyber conflict is taught to both lawyers and non-lawyers. The conceptualization of cyber conflict was highlighted as fundamental to bridging the gap between legal and technical experts whose interests overlap more often than their skill sets, but whose complementary and synergistic perspectives are essential to the nascent law of cyber conflict.

Format

The discussion was split roughly into two parts, mirroring the state of the field. "Tallinn 1.0" addressed issues that were the focus of the 2013 *Tallinn Manual*[46]. For the purpose of focusing on more specific research questions, gaps, and canonical works, within Tallinn 1.0, five different sub-topics were identified: (1) general work on *jus ad bellum* and its applicability; (2) key *jus ad bellum* sub-issues; (3) general work on *jus in bello* and its applicability; (4) key *jus in bello* sub-issues; and (5) sovereignty and neutrality issues not falling strictly into any one of the above *ad bellum* or *in bello* categories.

46 Written by an independent International Group of Experts, the *Tallinn Manual* examines how international law applies to cyberwarfare, taking the form of rules plus explanatory commentary. The *Tallinn Manual* pays particular attention to the *jus ad bellum,* the international law governing the resort to force, and the *jus in bello*, the international law regulating the conduct of armed conflict. *TALLINN MANUAL* ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (MICHAEL N. SCHMITT, ED., 2013).

The second half of the discussion looked "Beyond Tallinn[47]." This was roughly characterized as issues falling below the threshold for a use of force or armed attack in the *jus ad bellum* and which would not necessarily trigger application of the *jus in bello*. Participants identified four different sub-issues: (1) general work on cyber incidents below the traditional *ad bellum* and *in bello* thresholds; (2) governance, regulation, and norms; (3) cybercrime and cyber espionage; and (4) cyber terrorism and cyber sabotage.

Prior to the conference, the moderator and rapporteur prepared a list of canonical works for consideration. Works were grouped into the above sub-categories under the heading that best captured the work's main focus or most significant contribution to the pre-existing literature. Some were specifically highlighted during the discussion as examples of scholarship addressing one of the research questions. However, not every work included in the annotated list was considered individually by the conference participants. Based on the subjects discussed during the panel and follow-up consultations, the moderator and rapporteur have identified a smaller number of works from the initial list that may be considered part of the cyber law "canon[48]."

Early on in the discussion, the moderator and rapporteur clarified the standards used to compile the annotated list of works. The legal issues discussion was perhaps unique due to the role that formal legal sources play in legal analysis. Rarely is a single author, work, or school of thought the starting point for a legal analysis in the manner that those might be in, for example, the field of international relations[49].

---

47 Originally labeled as "Tallinn 2.0" at the time of the panel discussion. Discussions with those familiar with the Tallinn process clarified that while the original research agenda for Tallinn 2.0 envisaged a follow-up publication that covered a broader range of topics, the final Tallinn 2.0 Manual, to be published in December 2016, will address a more modest set of issues. It will contain updates and revisions to the original *Tallinn Manual* and will tackle a sub-set of issues on state responsibility. In subsequent years, additional follow-on manuals may continue to move along the spectrum of issues to cover progressively more of the field, an initiative welcomed by this panel's participants.

48 Participants expressed reservations about labeling works as canonical, fearing it may be premature to do so given the fluidity of the field and its relatively recent emergence as one receiving dedicated study by legal scholars. While this conference report has adopted the label of "canonical works," participants approached the task from the more modest perspective of what might be key works one would include in a syllabus covering the range of the field while giving a sense for the key debates which have informed its development.

49 (insert cross reference to discussion in the IR chapter of this report on, for example Waltz or Keohane)

Canonical works of law, if defined as those that first express or embody a key question or proposition and to which subsequent works must continually refer, might include treaty provisions, landmark judicial decisions, commonly accepted formulations of *opinio juris*, or state-issued interpretations of law, with perhaps only a few of the most historically important opinions of scholars included. For the purposes of determining the state of the field of cyber law studies, only works that had a direct focus on cyber conflict were considered as canon. Treaties like the UN Charter and the Geneva Conventions, landmark cases from the International Court of Justice (ICJ) or its predecessor[50] (such as *Nicaragua*),[51] cases from the International Criminal Court (ICC) or the *ad hoc* international criminal tribunals (such as *Tadic*),[52] statements from international bodies like the UN General Assembly and from groups of experts (such as the *Draft Articles on State Responsibility*),[53] military manuals of notable states (such as the United States Department of Defense's Law of War Manual),[54] or embodiments of customary international law (such as the *Caroline* Dictum or the Martens Clause)[55] were excluded from consideration for the as canon, though each is fundamental to understandings of cyber law.[56] Instead, the label "canon" was used more loosely to distinguish those works that have made a direct contribution to the relatively young field of the law governing cyber conflict. With a few notable exceptions, most are scholarly works.

There was some discussion over how to draw the line between those areas identified as existing research—where there is some basic level of consensus—versus those labeled as gaps, in which additional research would be useful. None of the issues were thought to be immune from future re-evaluation, based on changes in how actors operate in cyberspace or revisionist challenges to how the law should apply. For each sub-category, including those

50 [PCIJ citation with Lotus and Corfu Channel]

51 [Nicaragua ICJ citation]

52 [ICTY Tadic citation and include an ICTR and an ICC citation]

53 Draft articles on State Responsibility

54 Department of Defense Law of War Manual, 2015

55 [Caroline Dictum citation]; [Martens Clause citation]

56 Such sources are, however, cited extensively through the works designated as "canon" and can be found in the *Tallinn Manual*'s list of references

addressed at length in the *Tallinn Manual*, participants were able to highlight areas that have been underexplored or where there has been significant pushback against the prevailing view. For these areas, further scholarly exploration is needed. However, the participants agreed that for at least some issues, there is a baseline of consensus both among academics and among states and other significant actors operating in cyberspace, and for which further exploration is not an urgent priority. For example, the question of whether the *jus ad bellum* applies to cyberspace—at one time a focal point of research—has been well settled in the affirmative. Particularly in light of its treatment in the *Tallinn Manual*, the application of the *jus ad bellum* to cyberspace should be presumed in scholarship going forward. Revisiting the issue at length—not uncommon among those approaching cyber law issues for the first time—often ignores the substantial body of work that has previously addressed the issue.

This relates to a larger point one of the participants made about ambiguity and the law and how international law works. The conference highlighted that it may be tempting for those approaching the field from other disciplines to expect the law to provide unambiguous "rules of the road" for cyber conflict. This is perhaps best embodied by the common misperception that the *Tallinn Manual* can be considered a freestanding source of law.

The fact that law—particularly international law—is fluid is often underappreciated. Seemingly settled concepts can be overridden by subsequent law, may lose their binding nature through desuetude, can be subject to reinterpretation when an exception swallows the rule, or may simply not be applicable to the cyber context. Even for settled law, it is not always clear whether a violation undermines the law or honors it in the breach. The law governing cyber conflict is no different; those working on cyber conflict should approach the law with an appreciation for its inherent uncertainty. The emergent field of cyber conflict law is highly dependent on interpretation and implementation. Each new international cyber incident presents the potential for upending existing assumptions.

Further, the function of law is not always to provide certainty through the creation of clearly delineated, bright-line rules. Both for policy reasons and as a matter of practicality, the law often functions to preserve ambiguity and thus flexibility. Further, many of the legal issues surrounding conflict are hotly contested. In an example invoked by one of the participants, there is a robust, long-running debate about the level of imminence required to exercise pre-emptive self-defense. The debate exists both outside of and within discussions on self-defense in cyberspace. That the question is hotly contested and remains unsettled is thus not unique to cyber conflict. Whatever the basis, uncertainty in the law is something with which those approaching cyber studies

from a legal background tend to be familiar and comfortable. In contrast, participants had the general impression that those new to legal issues in cyberspace may initially find this uncertainty unsettling or may be prone to overstate the role of cyber capabilities in creating uncertainty.

While not comprehensive, the summary below highlights the key research questions and gaps for both halves of the discussion. Where appropriate, included are discussions of general or conceptual points that arose during the course of the discussion. Appended to this report is a list of proposed canonical works and an excellent resource for further study or the development of a research agenda.

Tallinn 1.0: *De lex lata* of cyberwar

The first half of the discussion reflected on the question that has motivated much early work on cyber conflict and the law: do traditional international law frameworks apply to activities in cyber space? A robust body of scholarship has examined the question in the context of both the UN Charter and related *jus ad bellum* frameworks and through the application of international humanitarian law and underlying *jus in bello* principles. That the debate has mostly been resolved through agreement that both major bodies of public international law apply to activities in cyberspace is a strong affirmation of the capacity of international law frameworks to cover new and emerging technologies. It also speaks to the utility of efforts like the *Tallinn Manual* process, which has sought to assess the law through a set of draft rules and accompanying commentary, a format familiar to legal scholars that lends welcome structure to the field. Participants noted that there is still a tendency for scholarship to unnecessarily return to the baseline question of whether international law applies to cyber activities. In the view of the participants, this evinces a need to build consensus not simply through the codification of the *Tallinn Manual*, but through greater awareness and diffusion of its content.

Participants generally felt that for each of the five sub-categories discussed, the most urgent research questions had been the subject of enough scholarship to establish a steady frontier of knowledge. They are also the most likely ground for scholars new to cyber law studies to re-tred in a way that fails to acknowledge the current state of the field.

However, for each area, participants also noted gaps that merit consideration for future research. For example, one participant noted there is still considerable uncertainty over how much of the Geneva Conventions states will accept as applying to cyber

operations, and thus more emphasis on actual state behavior in cyber operations would be helpful. Another noted that more could be done to differentiate between the "Hague Law" and "Geneva Law" branches of international humanitarian law as applied to cyber conflict. Another noted that *jus post bellum* might present a third field ripe for exploration in the cyber context, addressing issues of what responsibility actors might have to repair and remove themselves from adversary networks in the event of a conflict.

Participants emphasized the intermingling of legal and policy issues in trying to apply these standards in practice. One participant noted the importance of states asserting and proving that they have fallen victim to a cyberattacks as an example. States and observers may agree that a cyberattack can constitute a use of force in violation of the UN Charter and that a state may invoke its inherent self-defense rights to respond. But a host of policy issues dictate whether and how states choose to respond. Iran's failure to declare the Stuxnet operation a use of force or armed attack on its territory and the US response to the Sony hack were noted as examples where, despite agreement on general principles, state behavior may ultimately dictate the contours of what sorts of cyber operations trigger international law.

Another participant brought up the related point of how a state might go about persuading the international community of when, how, and by whom it had been attacked. That the highly technical nature of cyber operations are not easily understood by the general public, along with the attenuated timelines under which cyber operations take place and are discovered, may necessitate a re-thinking of how states prove an attack, which international institutions are seen as credible forums in which to present cyber evidence, and how long after an attack is discovered a state may reasonably respond.

Finally, participants noted a general concern that issues that appear settled may be challenged by revisionist powers looking to undermine the international law status quo. Questioning the application of *jus ad bellum* and *jus in bello* to cyber conflict may provide an entry point to challenge settled pillars of those bodies of law on a foundational level, feeding back into how their application is understood even as applied to conventional means of warfare.

The list of research areas and gaps addressed under each sub-category were:

Jus In Bello – General/Applicability

Research Questions:	General application of international humanitarian law to cyber operations.

Consideration of how the four core IHL principles apply to cyber operations in theory.

Conflict classification and cyber conflict.

Protections owed to the cyber-equivalent of humanitarian aid workers (CERTs, and other actors).

Gaps:

How much of the Geneva Conventions apply to cyber operations?

- Specific invocation of articles of the Geneva Conventions and core principles to cyber incidents as they arise.
- Focus on refusal of states to acknowledge application of various IHL principles to their conduct in cyber space.

Aside from CERTs, what types of persons, networks, and servers might qualify for protected status under IHL?

Jus In Bello – Secondary Considerations

Research Questions:

The principle of distinction as it applies in cyberspace.

Control of proxy forces may lead to responsibility for crimes committed in contravention of international humanitarian law.

Application of the presumption against targeting civilians and civilian infrastructure.

Agreement that standards for dual-use infrastructure may apply to networks.

Gaps:

Greater clarity on classification for infrastructure.

- Use of special markings or insignia for websites and servers (i.e., ".icrc")

Should any cyber-specific protections apply when cyber operations occur in the context of an existing armed conflict, or are pre-existing IHL protections sufficient?

Gaps:

How do states conduct necessity and proportionality assessments for cyber operations in practice?

Cyber conflict and the ongoing debate over the interaction between IHL and international human rights law.

Cyber-based violations of the laws of war and how to collect evidence, gain jurisdiction, and prosecute cyber war crimes, crimes against humanity, and aggression.

More on NIAC-specific concepts for distinction (i.e., DPH and continuous combat function).

Sovereignty and Neutrality

Research Questions:

States have sovereignty over their cyberspace. What levels of control over cyber infrastructure are required for sovereignty?

The international legal regime governing neutrality applies to cyberspace.

Certain uses of infrastructure may violate neutrality.

Doctrines of state responsibility apply to use of a state networks by nonstate actors.

Gaps:

Application of jurisdictional questions to cyberspace.

- I.e., territorial jurisdiction, passive personality, protective principle, and effects doctrine.

What is required for a third state to forfeit neutrality?

Exploration of effective versus overall control versus a third standard for actions taken by nonstate actors with the support or by direction of a state.

Government and private sector implications of state responsibility for misuse of infrastructure.

Beyond Tallinn: Cyber Incidents below the Traditional Thresholds

Participants generally agreed that issues falling outside the scope of the *Tallinn Manual* provide rich ground for further exploration and should serve as the focal point for emerging research agendas. Not only is there less clarity here on which law applies, but below-threshold incidents comprise the majority of cyber activities conducted by both states and nonstate actors. Like the proverbial iceberg, most of the field lies out of sight, below the surface. The relative secrecy surrounding many of these events presents a challenge for analysis. One participant noted the irony of how—despite concerns from the earliest days of cyber conflict studies that cyber operations would become increasingly more kinetic and violent—what has occurred in practice is a move towards less-kinetic activities. This may make the use of cyber capabilities more likely and more frequent, which in turn may increase the number of operations that do become known to the public either by discovery or by drawing a response from an affected party.

The four sub-categories addressed in the Beyond Tallinn portion of the discussion were: (1) general work on cyber incidents below the traditional *ad bellum* and *in bello* thresholds; (2) governance, regulation, and norms; (3) cybercrime and cyber espionage; and (4) cyber terrorism and cyber sabotage. The participants noted that while scholarly attention has begun to turn to the types of "post-Tallinn" issues that will need to be resolved to provide greater clarity on below-threshold incidents, the law on which these types of analyses rely provides a less-robust platform around which to build consensus. In many cases, there is no binding treaty law to look to for a written set of standards. In others, treaties are limited to a smaller set of signatories and it is not clear whether there is an appetite among states to replicate regional efforts on an international level, or to go beyond nonbinding codes of conduct.

Participants encouraged more scholarship on the content of what might go into an overarching cybercrime or otherwise cyber-focused treaty. One participant raised the example of the Budapest Convention as an example of an area where law exists that may provide a model for future treaty-making efforts, but whose reach is currently limited[57]. Another participant responded that the absence of treaty law would not necessarily hinder the development and acceptance of law for below-threshold events.

57 The Budapest Convention on the Prevention of Cybercrime (ETS No. 185), Council of Europe

The doctrine of sources, best expressed in Article 38 of the ICJ Statute[58], acknowledges customary international law, general principles, and the opinions of eminent jurists as additional sources of international law. While they may provide less clarity on the content of laws governing cyber activities below the threshold, it would be premature to believe that in the absence of binding treaties, no international law will directly apply to the activities in question.

One participant noted the role that domestic law, particularly in the United States, can play in setting standards for behavior in cyber space. Domestic law has been used successfully to penalize those who violate standards of conduct in cyberspace. The use of economic sanctions was mentioned as a possibility for further exploration, and another participant noted the use of criminal indictments against Chinese People's Liberation Army (PLA) members implicated in cyber espionage against Google and other private US-based corporations.

On the topic of clarity, the participants noted the need for more discussion on the legal distinction between cyber espionage conducted for traditional national security purposes and cyber espionage for private economic gain. In general, participants agreed that the way in which different sub-threshold cyber activities are defined is likely to be an enduring challenge. The initial determination of which body of law should apply may pre-determine the possible responses. Under US domestic law, determining whether to treat a cyber incident as espionage or an act of "cyber-terrorism" will determine which agencies may respond and what resources are at their disposal. Finally, participants noted that more work could be done on the confluence between cyber capabilities and influence operations, and whether the use of cyber capabilities to amplify influence and information operations changes how international lawyers should understand impermissible coercion in a state's domestic affairs.

58 Article 38, Statute of the International Court of Justice.

The list of research areas and gaps that were addressed under each sub-category are:

Cyber Incidents – International Law Below the Thresholds

Research Questions:

Which legal regime should apply to different categories of cyber incidents?

How might gaps between the legal regimes differentiating between war and peace account for the realities of cyber conflict?

How might particular cyber incidents be classified?

How do the laws on state responsibility apply to sub-threshold incidents?

Do doctrines that states may invoke in response to below-threshold events, such as countermeasures, apply in cyberspace?

Gaps:

General consensus on the law that applies for sub-threshold events.

Focused case studies that classify and contrast cyber incidents.

More on countermeasures and responses.

- What is the difference between a retorsion and a reprisal in cyberspace?

Governance, Regulation, and Norms

Research Questions:

How can states and international organizations govern and regulate cyber activity that falls below traditional force-based thresholds?

Is a cyber treaty or treaties the appropriate response?

- What might be the content of such agreements?
- How would they be policed and enforced?
- How would they account for nonstate actors?

What other normative or soft-law guidelines should govern activity in cyberspace?

How is the law governing cyber activity being formed?

What ethical considerations should factor into the development of law and norms for cyberspace?

Gaps:

For each of the above research questions, while initial concerns have been identified, more research is needed to delve deeper, build consensus, and offer alternative proposals.

Questions of institutional capacity and competences.

Cybercrime & Cyber Espionage

Research Questions:

What is the difference between cybercrime and cyber espionage?

- Between either and cyberwar?

What domestic law mechanisms can be used to deter and respond to state-sponsored economic espionage?

- Other forms of cybercrime?

What role for nonstate actors?

- Quasi-state actors?

Gaps:

More on the distinction between a crime-fighting model and a counterintelligence model of governance.

How should domestic law constrain or empower private entities in cyberspace to, for instance, "hackback"?

Distinguishing crime and espionage from sabotage and terrorism.

State practice and *opinio juris* based on case studies.

Cyber Terrorism & Cyber Sabotage

Research Questions:

What is cyber terrorism? What is cyber sabotage?

- Are they defined by their means, effects, or by intent of the parties?
- Must they have a primary purpose that is political (versus economic)? How do such acts differ from or follow the post-September 11 legal regime for countering terrorism?

Is cyber terrorism primarily useful to describe acts perpetrated by nonstate actors?

Gaps:

How to prosecute and combat cyber terrorism.

Attribution questions and support for proxies.

- What does attribution require? "What" versus "who" attribution.
- What does state-sponsored cyber terrorism look like? Does it include Advanced Persistent Threats (APTs)?

The role of the Dark Web.

Other roles for nonstate actors, i.e., white hats.

Information-sharing between states and between governments and the private sector.

Conclusion

In its relatively short history, scholarship on the law of cyber conflict has shown progress and promise. The debate over whether traditional legal frameworks govern cyber activities—the focus of much early work in the field—has largely been answered in the affirmative. Efforts like the drafting of the *Tallinn Manual*, the expansion of opportunities available to practitioners to engage with cyber law issues, and serious academic work examining a wide range of cyber law questions has created a strong foundation upon which to build.

Given the speed of cyber developments and how much cyber activity takes place out of the public view, any attempt to divide cyber conflict neatly into legal categories and sub-categories should be done with caution and be subject to periodic re-evaluation. The same lesson applies to attempts to portray cyber activities on a spectrum roughly equivalent to traditional law enforcement and military activities—with known thresholds distinguishing war and peace—around which the laws of conflict have developed.

As made apparent by the discussion, the "Tallinn 1.0" and "Beyond Tallinn" division and their subcategories are imperfect. It is not always clear when either *jus ad bellum* or *jus in bello* applies. Moreover, key issues in the field cut across the *ad bellum*/*in bello* divide, with many early works surveying cyber activities under both areas of law. Even below the threshold, it is not always clear when, for example, a cyber operation constitutes espionage or sabotage.

During the discussion, issues of significant import —like the role and obligations of nonstate actors—were not always broken out explicitly, but rather addressed within multiple sub-topics. This led to the critique that current cyber law scholarship often fails to acknowledge the uniqueness of cyber as a public domain with a backbone largely owned by the private sector, which provides an unusual amount of power and agency to private actors. This has significant implications for the ability of traditional international law means to regulate activities in cyber space through, for example, treaties, doctrines of state responsibility, and enforcement through international institutions. Recent scholarship has probed these issues to highlight the limits of understanding cyber issues through existing international law frameworks. Nonetheless, participants agreed that the categories used provided a generally useful framework and were consistent with the prevailing consensus that existing international legal regimes apply to the conduct of state and nonstate actors in cyberspace and should continue to serve as starting points from which cyber incidents are analyzed.

Participants acknowledged that cyber conflict is expanding, both qualitatively and quantitatively. More actors are involved in the domain and recent years have seen a constant evolution in the way that both state and nonstate actors use cyber capabilities to achieve strategic, military, diplomatic, and economic ends. As a result, cyber conflict continues to impact new areas of law. Untangling the implications of these changes requires scholars to apply current understandings of cyber law to events as they arise, creating a more robust set of case studies from which to draw lessons for the future.

Understanding the law that applies to cyber operations is essential. Precision and analytical rigor in scholarship on the law governing cyber conflict lends clarity to the larger field of cyber studies. Cyber scholars and practitioners should not expect the law to provide a set of bright-line rules or perfect clarity. Ambiguity is a natural part of the law and many of the issues that arise in cyber conflict are highly contested as a matter of general international law. Nonetheless, law may provide a common vocabulary, a background framework of regimes and norms, and a medium through which to translate lessons learned from other disciplines into enforceable policies. Fulfilling these potential benefits of cyber law research will require greater consensus among those working in the field and consolidation of lessons learned. Efforts like the inaugural State of the Field Conference and its follow-on efforts are steps in the right direction. •

IMPORTANT WORKS

Tallinn 1.0:

Michael N. Schmitt, Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

Horace B. Robertson, Jr., Self-Defense Against Computer Network Attack Under International Law, 76 INT'L L. STUD. 121 (2002).

George K. Walker, Neutrality and Information Warfare, 76 INT'L. L. STUD. 99 (2002).

Michael N. Schmitt, Wired Warfare: Computer Network Attack and International Law, 84 (846) INT'L REV. RED CROSS 365 (2002).

Louise Doswald-Beck, Some Thoughts on Computer Network Attack and the Law of Armed Conflict, 76 INT'L. L. STUD. 163 (2002).

Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE J. INT.'L L. 421, 429 (2011).

Sean Watts, Low-Intensity Computer Network Attack and Self-Defense, 87 INT'L L. STUD. 60 (2011).

Harold H. Koh, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012), in 54 HARV. INT'L. L.J. ONLINE 1 (2012).

Cordula Droege, Get off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, 94 INT.'L REV. OF THE RED CROSS 533 (2012).

REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, UN Doc. A/68/98 (June 24, 2013)

TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (MICHAEL N. SCHMITT, ED., 2013)

Terry D. Gill and Paul A. L. Ducheine, Anticipatory Self-Defense in the Cyber Context, 89 INT'L L. STUD. 438 (2013).

Heather A. Harrison Dinniss, Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War, in Dan Saxon, ed., INTERNATIONAL HUMANITARIAN LAW AND THE CHANGING TECHNOLOGY OF WAR (2013, Leiden: Martinus Nijhoff), 251–78.

Noam Lubell, Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?, 89 INT'L L. STUD. 252 (2013).

Michael N. Schmitt, Classifications of Cyber Conflict, 89 INT'L L. STUD. 233 (2013).

Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 89 INT'L L. STUD. 123 (2013).

Eric Talbot Jensen, Cyber Sovereignty: The Way Ahead, 50 TEX. INT.'L L. J. 273 (2015).

Beyond Tallinn:

Jack. L Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998).

Philip A Johnson, Is it Time for a Treaty on Information Warfare?, 76 INT. L. STUD. 439 (2002).

Charles C. Dunlap, Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy, 76 INT. L. STUD. 353 (2002).

Thomas C. Wingfield, "International Law and Information Operations," Ch. 22, CYBERPOWER AND NATIONAL SECURITY, (FRANKLIN D. KRAMER ET AL., EDS.) (Washington: NDU Press, 2009).

Duncan B. Hollis, An e-SOS for Cyberspace, 52 HARV. J. INT'L. L.J. 373 (2011)

Michael J. Glennon, The Road Ahead: Gaps, Leaks and Drips, 89 INT'L L. STUD. 362 (2013).

Michael N. Schmitt, The Law of Cyber Operations: Quo Vadis?, 25 STANFORD L. AND POL. REV. 269 (2014).

Gary D. Brown and Andrew O. Metcalf, Easier said Than Done: Legal Reviews of Cyber Weapons, 7 J. NAT'L SECURITY L. & POL'Y 115 (2014). Oren Gross, Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber Incidents, 48 CORNELL INT'L L. J. 481 (2015).

Kirsten Eichensehr, The Cyber-Law of Nations, 103 GEO. L.J. 317 (2015).

Gary D. Brown, Fighting and Spying in Cyberspace: What is Which? 8 J. NAT'L SECURITY L. & POL'Y ___ (forthcoming 2016).