COLUMBIA | SIPA
School of International and Public Affairs

CCSA
Cyber Conflict Studies Association

International Security and the Strategic Dynamics of Cyber Conflict

AUTHORS: Melissa K. Griffith and Adam Segal
SERIES EDITOR: Justin Key Canfil EXECUTIVE EDITOR: Jason Healey

Introduction

What is the state of the field of cyber conflict within the fields of international relations and international security? Which questions have been answered and which remain unexplored? Where should those hoping to push forward discussion around and promote an understanding of the strategic dynamics of cyberspace focus their intellectual energy and efforts? What are the questions scholars need to be asking now?

These were the driving concerns of the International Security and Strategic Dynamics panel at the 2017 State of the Field of Cyber Conflict Conference,[1] where researchers, policy analysts, and practitioners came together to discuss the emerging scholarship on cybersecurity. The goal of this particular panel, as summarized in this White Paper, was to capture the evolution of the field since the 2016 State of the Field Conference, to provide an overview of existing scholarship focusing on the strategic dynamics of cyberspace, and to identify where more rigorous research could expand the frontiers of the field.

The 2017 panel drew heavily on work completed by Ryan C. Maness and Adam Segal for the inaugural 2016 State of the Field Conference.[2] To assess the state of the field in 2016, Maness and Segal compiled traditional international security literatures and then looked for corresponding research emerging on cyberspace within those categories. The categories of interest were drawn from the foundational sub-literatures within international security, including deterrence, the offense-defense balance, security dilemmas, foreign policy doctrines, arms races, and norms or taboos. By mapping existing work onto these traditional security sub-literatures, Maness and Segal were able to identify emerging consensus and persisting disagreements and gaps. The questions asked in 2016 then became “what work has been done around deterrence,” “what are the limitations of this

About the State of the Field Series

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

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

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

approach," and "what gaps remain in the study of deterrence," rather than the far broader "what are the strategic dynamics of cyberspace?"

The 2017 panel first sought to update the research listed under these various categories to include work that had emerged over the preceding year and, second, to identify persisting gaps and potential limitations to this approach. In addition to newly published work, we also considered presentations at the 2017 International Studies Association (ISA) Conference as markers of unpublished work in progress by scholars.

Notably absent from this White Paper's analysis, however, are the bodies of work addressing intelligence, economics, operational and tactical dynamics, the history of cyber conflict, and the legal and ethical issues embedded within cyber conflict. Each of these topics, given its importance to the field of cyber conflict and security research, comprised its own panel and subsequent White Paper. Similarly, work focusing on cybercrime, although a subset of the cyber security debate, remains outside the scope of this project. Given the conceptual distinctions drawn between White Papers and between cyber conflict and other forms of cyber incident, this White Paper specifically focuses on strategic dynamics by mapping out the relationship between the strategic study of cyber conflict and the foundational sub-literatures within international security. It leaves the analysis and review of these related bodies of work to others.

Many of our findings are consistent with the trends identified in 2016. Articles continue to be heavily focused on larger states (e.g. the U.S., the U.K., China, and Russia). In terms of theoretical frameworks, the categories of deterrence and offense-defense balance represent the largest bodies of work. Certain sub-fields that receive significant attention in other security domains, such as international cooperation, remain systematically understudied. Finally, an overarching refrain during the plenary discussion was a continued questioning of whether international security and its sub-literatures provide useful analytical leverage for studying the strategic dynamics of cyber security, whether important dynamics remain uncaptured, and whether more progress could be made through greater reliance on analytical tools from other disciplines. This debate was reflective of the fundamental question of whether cyberspace has created a revolution for security politics or whether some aspects of previous security politics remain relevant for the study of cyber security.

Given these findings, we conclude that progress in the field remains slow and evolutionary. Within the field of international security, several key gaps remain. Moreover, as in other political science fields, there is a sharp divide between practitioners/policy analysts and academics on the utility and applicability of units of analysis, theories, and methodologies drawn from international security studies.

This White Paper will proceed in three parts. First, we will discuss the major takeaways from the 2017 panel discussion. This section will focus on the overall structure of the field and emerging oversaturation and gaps within it. Second, we will outline the current state of the field. This section will break existing work into sub-categories, or sub-literatures, and tie those works directly to questions currently being asked while highlighting unanswered questions that have persisted within and between categories. While this section of the paper does not act as a comprehensive literature review of work on the strategic dynamics of cybersecurity, we hope it will be a useful foundational reference for those entering the field. Throughout, we will strive to identify new work rather than simply recapping the work already covered in the 2016 State of the Field Report. Third, we will provide a short summary of key observations from our preparation and the subsequent panel discussion, identify limitations of the approach used to develop the panel and this paper, and provide a few recommendations for moving the field forward.

Major Takeaways from 2017

During our preparation for this panel and in the subsequent panel and plenary discussion, four key takeaways emerged: tensions remain between academics and policy practitioners regarding the utility of international security studies to cyber security research; the field continues to over-study some topics and ignore others; there is a high degree of overlap between the panels on tactical/operational dynamics and those on strategic dynamics; and there is a need to better link the destructive or disruptive effects of cyberattacks with the strategic goals states pursue in cyberspace.

First, the utility and applicability of international security studies and international relations more broadly remain contentious, especially between practitioners/policy analysts and academics. The main concerns here point to diverging intellectual interests. These fields bring with them assumptions about which variables are most influential and which dynamics are most important in the study of conflict. For example, international security and international relations focus heavily on states. Yet the state is only one of many actors in cyber conflict, and the private sector in particular plays a large role. This discussion left us once again with a question voiced last year: in what ways might traditional security discussions and theoretical frameworks limit discussion of cyberspace and its strategic dynamics?

Second, the same areas continue to be studied. Gaps identified in 2016 largely persist. Empirical work and case studies focus on a select few countries.

Given these dominant topics and persisting gaps, why has the field developed in the manner in which it has? Why, for example, do we see a heavy, persistent focus on deterrence and the offense-defense balance and, simultaneously, a hesitance to address cybersecurity using other sub-literatures within international security?

Is this merely a question of timing? After exploring preliminary questions through the dominant sub-literatures, will scholars move on to the additional sub-literatures? This would almost seem to imply that there is a natural progression for any topic located within international security. Certain dynamics may be studied before others because the concepts addressed are building blocks for later sub-literatures, because the outcomes inherent to some sub-literatures occur historically later than outcomes studied in others, or because the prioritized sub-literatures are dominant in the broader field of international security.

Perhaps it is a question of applicability, especially for policymakers and practitioners. However, the applicability of deterrence and offense-defense balance to this new threat space is highly contested. Much of the debate after our panel focused on moving away from deterrence models because they were not applicable.

The core observation remains: the evolution of the field is largely consistent. The question as to why remains unanswered and underexplored.

Third, clearly delineating between tactical, operational, and strategic levels of war in cyber conflict is easier in theory than in practice. While conceptually the State of the Field Conference separated tactics and operations from strategic dynamics, in the subsequent discussions for both sessions there was significant overlap.

This overlap may have been due in part to an open forum format conducive to the blurring of boundaries or the way some topics—such as work focusing on how standard operating procedures shape strategic cyber planning—naturally bridge buckets. But the more interesting explanation is the particular challenge cyber conflict poses to the levels of war categorization. The issue here is not the more general point that the dynamics in one level affect dynamics in another but rather that in cyberspace, dynamics at the tactical level increasingly reverberate at the strategic level. In cyber conflict, including cyber-facilitated information operations, "analysts face the challenge of the strategic corporal in a more dramatic fashion: tactical behaviors can rapidly have strategic effects."[3] Given these dynamics, questions of interest reside between levels of war rather than in discrete buckets more often here than in the study of conflict on air, land, and sea.

Why, then, should scholars keep a levels of war distinction? There are several advantages to utilizing this conceptual distinction for research in international security and the strategic dynamics of cyberspace. First, there are different dynamics at each of these levels worthy of study. Take the dynamic of speed as an example. At the tactical level, things occur at the speed of light with very little reaction time, but at the strategic level, campaigns are more prolonged. Second, the levels of war provide a useful frame for understanding particular outcomes. Take the cyberattacks on Estonia in 2007 as an example. Tactically, Estonia lost, with widespread outages in the face of massive DDOS attacks. Strategically, Estonia still moved the statue and has, over the last decade, used the attacks to establish itself as a leader in cybersecurity and international norms.

This third takeaway from the 2017 Strategic Dynamics panel points to the need for additional attention to be paid to the ways in which cyber conflict blurs traditional conceptual boundaries utilized in other security domains. When do levels of war remain distinct and productive categories? When do these categories limit inquiry into the dynamics of cybersecurity?

Fourth, this panel merged two previously distinct panels: international security and strategic dynamics. In addition to increasing the range of relevant literature and potential research questions, these overlapping fields do have two distinct framings. In some contexts, we are focusing on the destructive effects of conflict. In others, the outcome of interest is not destruction but rather the strategic effects. These are not one in the same. To grapple with the strategic dynamics of this space, we need to frame discussions around the strategic outcomes motivating and/or driving conflict. These focuses lead to two very different sets of questions: (1) what are the dynamics or core characteristics of cyber conflict, and (2) how do specific actors pursue strategic outcomes using cyber means?

2017 State of the Field: International Security and Strategic Dynamics of Cybersecurity

There are many different ways to conceptualize a "state of the field." When we ask what work is missing, what questions have been asked, and what questions need to be asked, the intended target audience should be at the forefront of any discussions. Different audiences require different information and often hold different research goals and desire different deliverables. These diverging preferences were on full display at the 2017 State of the Field Conference, which brought scholars, policy analysts, and practitioners together to grapple with a research agenda for cybersecurity.

What, then, do we mean when we identify gaps in the literature and posit from these gaps what the next wave of research questions should be? Is this research directed at policymakers tasked with developing cybersecurity policy, PhD students pursuing an academic career, or scholars contributing to their chosen field? While there is some overlap thematically between these three audiences, the exact research questions vary.

This panel, like that of 2016, focused on the second and third categories and compiled resources to that end. We recognize, however, that the state of the field—work completed and remaining gaps—would be organized differently for policymakers or policy analysts. Moving forward, research on the areas of overlap between the academic and policy communities may be the most fruitful.

Our 2017 review of the state of the field is organized around eight subtopics of cyber conflict and security within international security. These subtopics are not mutually exclusive, and many overlap. Indeed, some subtopics include broadly grouped work, a byproduct of the limited research available in these areas. As more research is pursued, these broader categories can and should be broken apart into their constituent parts. The subtopics are as follows:

1. The Structure of the Security Environment: Defining the Degree of Change
2. Deterrence, Dissuasion, and Attribution
3. Offense versus Defense, the Security Dilemma, and Escalation
4. Power and Influence
5. Foreign Policy and Doctrine
6. The Relationship between State and Non-State Actors
7. Norms and Norm Diffusion
8. International Institutions and Cooperation

We take each of these eight categories in turn, providing a short summary followed by relevant works and key questions. The conclusion of the section captures the questions that emerged in the subsequent panel and plenary discussions. Where applicable, subsequent panel discussion questions have been folded into their relevant bucket. After reviewing the subtopics, we draw attention to a range of concerns that do not fall as neatly into a single category.

It is worth noting that although we organize this White Paper thematically, there is an alternative chronological framing. Scholarship in the 1990s and early 2000s focused heavily on the Revolution in Military Affairs (RMA) and how information technology altered the ways in which wars were fought and conflict was conducted.[4] This scholarship largely gave way to research focusing on the broader implications of technological shifts for conflict and war in the international system.

Research from the early to mid 2000s focused heavily on the structural implications of cyberspace: whether potential cyber conflict represented an evolution or a revolution in the nature of warfare. By the late 2000s and early 2010s, academics had begun to move beyond structural implications and into research on the specific strategic dynamics of conflict, such as deterrence, compellence, offense-defense balance, cooperation, and norms development. This uptick in interest within international relations and international security will likely lead to additional phases of research that move into categories of inquiry so far overlooked.

The Structure of the Security Environment: Defining the Degree of Change

A debate from the 2016 conference that carried forward into 2017 is whether cyber conflict represents a revolution or an evolution of conflict.[5] If it is the latter, previous theoretical models more readily describe the phenomenon. If it is the former, then many, if not most, of our theoretical models contain assumptions and dynamics that are inappropriate to the study of cyber conflict and cyber security.

While it is easy to simplify this discussion into an "everything has changed" and "nothing has changed" caricature, it is more useful to ask: Which aspects have changed? By how much? What has remained the same? How similar? Given these changes to the structure of the security environment, what are the strengths and limitations of our current models?

Early scholarship examined the future of the Internet as a domain of conflict, worst- and best-case scenarios in cyberspace, and whether the structure of the "5th domain of warfare" radically departed from previous security domains.

In the 2016 report, this discussion was housed, in part, under "Opening Concerns with IR Categories" and "How Does Cyber Fit into IR." Surveyed work included Arquilla and Ronfeldt (1993), Clarke and Knake (2011), Choucri (2012), Junio (2013), Kello (2013), Lawson (2013), Rid (2013), and Lindsay and Kello (2014).[6] Additional works published within the last year include Kello (2017), Lindsay (2017), and Perkovich and Levite (2017).[7]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around the structure of the cyber security threat environment. We highlight two here:

1. How should we characterize the structure in relation to other security environments? What models best capture cyber security and conflict?

1a. How does the structure compare to other security environments?

The purpose here is to identify similarities and differences between a range of security environments and then to determine which of these similarities and differences most influence the structure and outcomes in this space. How does the structure compare across other warfighting domains (air, land, and sea)? Is it more or less escalatory? Does the central role of the private sector make cyberspace fundamentally different from other domains? Does the range of actors and their relative power differ? Is conflict less discrete here than in previous threat spaces?

1b. Which models can we draw on beyond those used for other warfighting domains? What are the limitations of state-centric kinetic force models?

There was strong consensus in the room over the clear limitations of international security models. In the panel discussion, several audience members raised concerns over the kinetic force assumptions built into much of international security studies. They pushed instead for a focus on other types of scholarship geared around non-security systems. Suggestions for bodies of work that might better capture the structure of this threat space included human security, public health,[8] and economics.

In addition, it would be useful to move beyond state-to-state behavior and toward systems behaviors. We know that non-state actors (individuals, corporations or firms, terrorist organizations, etc.) play a significant role in cyber conflict and security. There are international relations sub-literatures that focus on a wider range of actors. We should more readily draw on sub-literatures including terrorism, intrastate conflict, and organized crime in our work on cyber conflict. Furthermore, we could utilize system-based or network analysis-based approaches to mapping out the underlying structure of cyber conflict.

2. Examining structure is useful for developing research on cyber conflict, especially as

it relates to international security. But what is the nature of the relationship between the structure and the ways we are organizing within this domain?

One thread of the panel discussion focused on exploring the structure of cyberspace and cyber-facilitated conflict: the underlying dynamics that all actors in this space face. Two sub-questions animated this discussion. First, what organizations are emerging from the structure? Second, how do those organizations affect the structure itself? These two questions point to a desire to move away from unidirectional cause and effect thinking in this space. Rather, structure shapes organizations and organizations can in turn shape the underlying structure. This process is iterative. We need to move beyond conversations on structure alone and assumptions that it is independent of efforts to grapple with this new threat space.

Deterrence, Dissuasion, and Attribution

Consistent with the 2016 report, deterrence remains an area with comparatively significant coverage. However, given the perceived limitations of the deterrence model, it has been suggested that discussions should be rooted in the fundamental characteristics of cyberattacks and conflict; this is a non-kinetic space defined by continuous rather than discrete conflict, where attribution is difficult and non-state actors are increasingly important players. Addressing these characteristics will likely require us to look beyond deterrence and toward models of dissuasion, compellence, bargaining, and restraint.

In the 2016 report, surveyed work included Kugler (2009), Libicki (2009), Goodman (2010), the National Research Council (2010), Nye (2011), Cooper (2012), Valeriano and Maness (2014), and Gartzke and Lindsay (2015).[9] Other notable works published prior to 2017 include Harknett (1996), Clark and Knake (2010), Liff (2012), Tsagourias (2012), Gartzke (2013), Iasiello (2013), Schmitt and Vihul (2014), Lindsay (2015), Healey (2016), and Lupovici (2016).[10] Additional work published in this category within the last year includes Borghard and Lonergan (2017), Chen (2017), Davis et al. (2017), Edwards et al. (2017), Fischerkeller (2017), Harknett and Fischerheller (2017), Harknett and Nye (2017), Mandel (2017), Nye (2017), and Sharp (2017).[11] Papers and posters on this topic at ISA 2017 include Cunningham, Lupovici, and Wilner.[12]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around deterrence, dissuasion, coercion, and attribution. We highlight four here:

1. How can you deter a cyberattack?

This question was highlighted in the 2016 State of the Field Conference, persisted in the 2017 panel, and continues to animate policymakers and academia.

There is widespread agreement that cyber conflict raises specific challenges for classical models of deterrence. Classical deterrence relies on (1) a credible threat of the imposition of costs in retaliation (deterrence by punishment), and/or (2) the ability to deny strategic benefit (deterrence by denial) if an attack does occur. These mechanisms for deterrence face unique challenges in cyberspace for four broadly discussed reasons (see Libicki (2009), Iasiello (2013), and Rid and Buchanan (2015)).

First, attribution presents a unique challenge in cyberspace. Complexities include the time it may take to technically or politically attribute an attack to a specific actor; difficulties raised by false flags, plausible deniability, and proxy actors; and reliance in some instances on private actors for forensic attribution. Attribution can be more or less challenging depending on the type of cyberattack in question and the resources a state can bring to bear.

Second, reliance on cyberspace is asymmetric. Some states and non-state actors have smaller relative attack surfaces than others, limiting the potential scope and scale of retaliation in kind. In contrast with nuclear weaponry, to which all states are vulnerable, potential adversaries may not be equally vulnerable to cyberattacks.

Third, the difficulty of signaling cyber cost-imposing capabilities further complicates matters. Cyber capabilities are less visible than their kinetic counterparts and have limited life spans (i.e., once attacked, the target is made aware of a vulnerability and has an opportunity and incentive to address it).

Fourth, proportionality or retaliation requires proper categorization of an incident and tailoring of a proportional response. In the cyber realm, however, the purpose and scale of an attack is often ambiguous. An observable outcome could be a failed effort at a more major network breach, a warning shot, espionage, or an operational preparation of the environment (OPE) for future activity. On the other side of the coin, the effects from any given attack can be unpredictable and can far exceed the root cause. Taken together, these four challenges undermine the ability of states to credibly threaten the imposition of costs in retaliation and to signal their capability of denying the benefits gained from cyberattack.

While there is consensus over these major challenges to deterrence, there is little agreement in the literature about whether or not these challenges can be overcome. Several scholars argue that despite these limitations, deterrence is still possible in cyberspace. Gartzke and Lindsay (2015), for example, focus on cross-domain deterrence and argue that ways of imposing costs beyond punishment in kind can overcome concerns around asymmetry and signaling. Goodman (2010) contests that deterrence is harder in theory than in practice, while Nye (2017) draws attention to the array of deterrence mechanisms beyond punishment and denial: entanglement and norms/taboos. Others have proposed entirely new models of managing potential cyber aggression that move away from deterrence entirely. For example, Harknett and Fischerkeller (2017) argue that, given its limitations, deterrence is not a credible strategy for cyberspace, and that we should turn instead to a strategy of cyber persistence.

Ultimately, much of the work focusing on how states can deter cyberattacks or best manage those attacks that do occur remains largely theoretical. It has yet to delve deeply and systematically into empirical analysis focusing on instances of and strategies for deterrence in this space.

2. How critical is attribution to deterrence?

Early scholarship and opinion pieces on deterrence in cyber conflict focused on the central role of attribution and the ways in which it is slow or imprecise in this realm. Rid and Buchanan (2015) and Libicki's (2016) work rests here. Research questions in this vein begin with the role that attribution plays in deterrence models, then spiral out into the types of attribution that are possible within the context of cyber conflict. From there the question becomes, given these particular dynamics of attribution, is it possible to utilize traditional deterrence models? What are the limitations of deterrence in this context? Nye (2017), for example, argues that deterrence and dissuasion in cyberspace are comprised of four mechanisms and that only the first—threats of punishment—requires attribution.

Moreover, attribution is not merely a technical act. Edwards et al. (2017) highlight the differences between the strategic and technical components of attribution, as well as reasons why states might choose not to undertake it. In a similar vein, Healey's (2016) attribution scale as well as the work of Rid and Buchanan (2014) and Davis et al. (2017) provide foundations for attempts to move away from technical forensics around attribution and toward more political determinations.

3. How relevant is the nuclear deterrence model to cyber deterrence?

There was widespread agreement during this panel that the nuclear model does not provide useful leverage for deterrence in the context of cyberattacks. This past year, for example, Chen (2017) argued that we need to move away from the nuclear model of punishment and denial and toward a model focusing on engagement and surprise. The limitations of the nuclear model range from a focus on state actors to attribution to credible punishment. Many of these same limitations apply to deterrence models more generally. For example, Fischerkeller (2017) argued for an offensive component to cyber deterrence, and U.S. General James Cartwright referenced the importance of demonstrated offensive capabilities to deterring adversaries.[13]

In addition, Clark and Knake (2010) highlighted the limitations of the nuclear model for deterrence, given that it rests on large scale retaliation in kind and assumes total prevention of nuclear attacks. In cyber conflict, retaliation may not be in kind and both the attack and response may fall below thresholds of war. Moreover, in a domain of constant contact, total prevention is not the goal of any defense strategy. Rather, states should focus on preventing escalation beyond low-level activity and maintaining society-wide cyber resilience.

4. What are the persisting limitations of deterrence models? Given those limitations, what alternative models should we utilize?

These types of questions represent the most vibrant paths forward for deterrence research. Deterrence, or at least the punishment model, may be a dead end for cyber conflict studies, but broader questions regarding conflict mediation and prevention remain central and productive areas of inquiry.

Should we use kinetic literatures to analyze the strategic dynamics of a non-kinetic space? How applicable are theories of deterrence to a threat space defined by constant, rather than discrete, conflict? Given these defining characteristics, what alternative models might apply to conflict prevention in cyberspace?

Four potential alternative approaches were suggested during the panel discussion: dissuasion, compellence, bargaining, and restraint. Notably, Gartzke and Lindsay (2015), Valeriano and Maness (2015), Harknett and Fischerkeller (2017), and Nye (2017) all provide alternative models to deterrence in their work. During the panel discussion, it was also suggested that we should look to scholarship like Fearon's work on bargaining and cooperation for inspiration.[14]

In conclusion, it would be productive to move away from literatures focusing on conflict as either on or off, and into conflict management and prevention strategies resting on understandings of conflict as continuous.

Offense Versus Defense, the Security Dilemma, and Escalation

Consistent with the 2016 report, offense versus defense and the security dilemma continue to garner significant coverage. The core assumption of work cataloging the offensive and defensive characteristics of cyberspace is that these characteristics drive the likelihood, intensity, or cost of conflict. Existing work has been motivated by two broad questions: (1) is cyberspace offense or defense dominant, and (2) what factors determine whether cyberspace is offense or defense dominant? Newer work has begun to challenge the technological determinism endemic to the study of cyber conflict and apply instead reframe the existing theory these lessons to a broader security dilemma discussion and to the dangers of escalation. This emerging literature could be expanded further still, to include more empirical work and a greater focus on the differences between the strategic dynamics present in offensive and defensive efforts.

In the 2016 report, surveyed work included Andres (2012), Liff (2012), Fielder (2013), Gartzke (2013), Peterson (2013), Saltzman (2013), Rid and Buchanan (2014), Valeriano and Maness (2014), and Gartzke and Lindsay (2015).[15] Other notable works published prior to 2017 include Libicki (2007), Lin (2010), Lin (2012), Malone (2012), Fielder (2013), Kello (2013), Lieber (2013), Lindsay (2013), Rid (2013) and Harknett and Goldman (2016).[16] Additional works published within the last year include Buchanan (2017), Slayton (2017), and Smeets (2017).[17] Papers and posters on this topic at ISA 2017 include Buchanan, Loleski, Monte, and Slayton.[18]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around offense versus defense and the security dilemma. We highlight three here:

1. Is cyberspace offense or defense dominant?

What factors determine whether cyberspace is offense or defense dominant? Does a theory built around the relative ease of holding or taking physical geographic territory make sense when applied to cyberspace?

There is widespread support in academic and policy circles for viewing cyberspace as offense dominant (e.g. Libicki (2007), Nye (2010), Liff (2012), Kello (2013), Lieber (2013)). However, a vocal minority (e.g. Lindsay (2013) and Rid (2013)) is pushing back against the claim that offense has the upper hand.

Embedded within the question of whether offense or defense has the upper hand is a series of arguments around how to determine or measure this balance. One subgrouping of scholars (e.g. Malone (2012) and Saltzman (2013)) assesses the relative costs of taking versus holding cyber territory to determine the offense-defense balance, while others (e.g. Buchanan (2017)) examine whether offensive cyber operations have a first-mover advantage. Additionally, some scholars tie their arguments around the primacy of the offense directly to the challenges facing deterrence in cyberspace (see previous section of this White Paper). In their efforts to determine the balance, however, Gartzke and Lindsay (2015) distinguish between ease of deception and ease of attack in cyberspace. This distinction proves important, as they argue that, while these two dynamics are often conflated, the former's impact on the offense-defense balance remains largely uncertain.

Scholarship on the cyber offense-defense balance has not been limited to the cyber domain. Gartzke (2013), for example, posits that offense dominance in cyberspace corresponds with defense dominance in terms of kinetic conflict and physical territory by illustrating an inverse relationship between the two domains. Goodman (2010), Andres (2012), Gartzke (2013), Lindsay (2013), and Valeriano and Maness (2014) also highlight that while offense may dominate in cyberspace, this balance likely does not affect the broader balance of power in the international system.

More recently, Slayton's (2017) work seeks to move away from the largely shared assumption that cyberspace is offense dominant. Slayton argues that the costs of cyber operations are determined by organizational skills and capacity rather than some quality intrinsic to the technology itself. As such, we should move away from the dominant approach of conceptualizing this balance in terms of technology and toward skilled practice.

As technology moves forward, however, interest in using offense and defense categories for classification and analysis persists. For example, Frank L. Smith III, a senior lecturer at the University of Sydney, has sought to apply the offense-defense balance to his work on quantum computing.[19]

2. How should we characterize the security dilemma in the context of cyberspace?

Compared to the debate around offense-defense dominance in cyberspace, this area remains largely understudied. At ISA 2017, two presentations focused on questions around the security dilemma: Loleski and Buchanan. Buchanan (2017) also published a book this past year examining the cybersecurity dilemma, with a particular focus on its mitigation. Earlier work in this area focused on select aspects of these dynamics, such as deception (Gartzke and Lindsay (2015)), cyber posturing (Saltzman (2013)), offensive cyber weapon acquisition and deployment (Smeets (2017)), and escalation (Lin (2012) and Fielder (2013)).

3. Do the strategic dynamics of cyberspace differ between offensive and defensive efforts? If so, how?

We need to decouple offensive and defensive conversations around cyber conflict, since the dynamics present in one may very well differ from the dynamics present in the other. In the panel discussion, two dueling narratives emerged. On the one hand, powerful states dedicate billion-dollar budgets and make constant calls for more resources and money to develop their cyber capabilities. On the other hand is the single actor, such as a teenager successfully hacking NASA. North Korea is becoming an active and sometimes very effective actor in cyber conflict. The first example seems to support the narrative of cyberspace favoring traditionally strong actors. The second and third examples support the narrative of cyberspace challenging traditional definitions of power. Does cyber conflict favor the strong and powerful? Or does it empower a wide variety of actors? In other words, is cyber power centralized or diffuse? And given that the latter examples are largely offensive in nature, does the answer differ when talking about offensive versus defensive aspects of this threat space?

As for other sub-categories discussed in this White Paper, work on the offensive and defensive characteristics of cyber conflict and resulting security dilemmas is highly theoretical and would benefit from more empirical study and focus on cases outside of the U.S., Russia, and China.

Power and Influence

What is cyber power, and how can we measure it? What does "net assessment" mean in cyberspace? What qualifies as influence in cyberspace, and how can we measure it? Is cyber power soft or hard power, or both? These are the types of questions that animate the emerging literature on power and influence in cyberspace.

In the 2016 report, surveyed work included Rattray (2001), Libicki (2007), Kramer (2009), Nye (2010), Betz and Stevens (2012), Rid and McBurney (2012), Sheldon (2012), Healey (2013), Lindsay (2013), and Segal (2016).[20] Other notable works published prior to 2017 include Kramer et al. (2010), Klimburg (2011), Betz (2012), Ebert and Maurer (2013), and Sheldon (2014).[21] Additional works published within the last year include

Borghard and Lonergan (2017), Kello (2017), Maurer (2017), and Sharp (2017).[22] Papers and posters on this topic at ISA 2017 include Langø and Maness.[23]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around power and influence. We highlight three here:

1. How much of a role does soft power play in cyber power?

Discussion during the panel focused on how to categorize cyber power within the soft power-hard power divide. Stuxnet, often regarded as the world's first cyber weapon, destroyed Iranian centrifuges used to enrich uranium. Information warfare deployed during the 2016 U.S. election targeted public opinion in key demographics. These are both examples of cyber conflict, yet the former falls more neatly into traditional conceptualizations of hard power, while the latter is an example of psychological and information warfare and the use of soft power. Given the plethora of work from the last year on cyber coercion (Borghard and Lonergan (2017), Sharp (2017), and both Langø and Maness at ISA 2017), does it make sense to think of cyber coercion as largely hard or soft? Empirically, what have been the most prevalent forms of coercion in the past? Is this likely to change, and under what conditions?

2. How do we measure cyber power?

One potential definition of "cyber power" is the ability to inflict damage on adversaries and defend against outside attack. Though this categorization of the definition could be taken to apply to any form of power. But the relationship between capabilities and vulnerabilities is complex in cyberspace. The U.S., for example, is simultaneously one of the most capable and one of the most vulnerable countries in cyberspace. North Korea is both capable and largely disconnected, leaving it with few vulnerabilities. As these examples demonstrate, power in the cyber realm must be more than a ratio between capability and vulnerability.

Within existing scholarship, efforts have been made to categorize different elements of state cyber power. Take, for example, the following two notable frameworks. In their book, Betz and Stevens (2012) identify four types of cyber power: (1) coercion to modify behaviors of another actor, i.e. "compulsory cyber-power"; (2) control over a cyberspace actor through institutions, i.e. "institutional cyber-power," (3) maintenance of the overall structures, or network society, in which all actors are embedded, i.e. "structural cyber power"; and (4) the production and dissemination of discourse through cyberspace, i.e. "productive cyber power." In contrast, and looking specifically at the state, Klimburg (2011) breaks cyber power down into three different components: (1) operation and policy coordination within the state, i.e. "integrated government capability"; (2) coherent policy within international institutions and agreements, i.e. "integrated systems capability"; and (3) cooperation with non-state actors, i.e. "integrated national capability."

As part of the discussion about defining cyber power, scholars are also grappling with the theoretical and empirical task of measuring it. As explicitly discussed in the 2016 State of the Field report, "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?"

3. In what ways does cyber power alter the broader distribution of power?

We often speak of cyber power in isolation from other forms of power, but how do they combine across domains? Is it merely additive? Are particular forms of power in other domains undermined by a lack of cyber power? Can they directly determine levels of cyber power? Take, for example, arguments that correlate economic and private domestic industry strength to components of cyber power. The U.S. and Israel are commonly cited in this type of analysis, but in the context of security policy, highly networked militaries like that of the U.S. also face significant cyber vulnerabilities. In this instance, a certain level of cyber power is required to ensure the continued utility of other forms of power. Given these complex interrelations, how, from an empirical and a theoretical standpoint alike, can we measure the relationship between various forms of power?

We care about power because it is the central currency of international politics. Power, influence, and coercion all allow actors to pursue outcomes they desire. The focus then becomes the ways in which cyber power and the distribution of power alter the broader ability of states and other actors to pursue or achieve their strategic goals. Cyber power and politics are not independent of the broader geo-strategic positions of the states themselves. Consistent with this view, Ebert and Maurer (2013) highlight how, with the economic rise of the BRICS and increasing divergence between U.S. preferences and those of Brazil, Russia, India, China, and South Africa, cyberspace has become increasingly contested.

Can cyber power alter broader balances of power in international politics? Betz (2012) argues that the effect of cyber power on the international balance of power is relatively small, which is consistent with the views of scholars arguing that the offensive dominance of cyber space is unlikely to significantly alter the balance of power (see previous section). Nye (2010) looks at the diffusion of power in cyberspace but similarly concludes that this diffusion should not be mistaken for equal distribution.

In his 2017 book, Kello identifies three types of shocks, or "revolutions," occurring in international relations due to the introduction of cyber conflict. First, it empowers new actors and challenges the supremacy of states as the fundamental building blocks of the Westphalian system. Second, it empowers a new set of "revolutionary states," and through a shift to the balance of power alters the order of international politics. Third, it presents entirely new dynamics of engagement between actors and/or states that, in turn, alter our understanding of dynamics such as deterrence and the offense-defense balance. Kello's breakdown of the three levels of shocks now impacting international relations raises the question, which actors are empowered by this process and which are disadvantaged? How has it altered the types of tools these actors need to deploy in international politics to maintain power or influence? How might these shocks to pre-established distributions alter the overall balance of power?

Persisting gaps in the broader literature include the ways cyber power interacts across domains and the role it plays in broader global distributions of power for state and non-state actors. In both queries, the question of how to measure power and changes in power remains a central and critical challenge.

Foreign Policy and Doctrine

How do cyber operations impact foreign policy? What shapes the foreign policy doctrines of specific actors? In 2016, this was one of the most dynamic discussions during the panel. In 2017, our focus on this topic moved toward the states that remain outside the emerging literature and analysis. As was reported in the 2016 report, few in-depth studies of cyber operations impact on decision makers exist. Existing studies focus on the U.S, Russia, China, Israel, and the U.K., leaving gaps for theoretical and empirical work within this sub-category of research.

Work surveyed in the 2016 report includes Cavelty (2007), Gvosdev (2012), Reveron (2012), Guitton (2013), Inkster (2013, 2016), Junio (2013), Segal (2013), Axelrod and Iliev (2014), Gompert and Libicki (2014), Lindsay (2014), Geers (2015), Jaitner and Mattson (2015), Lindsay, Cheung, and Reveron (2015), Kaplan (2016) and Maness and Valeriano (2016).[24] Additional works published within the last year include Inkster (2016).[25] Papers and posters on this topic at ISA 2017 include Barrinha and Renard.[26]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around foreign policy and doctrine. We highlight four here:

1. How do leaders make decisions around cyber conflict? Which heuristics are useful?

How have different states approached cyber foreign policy and how are they developing cyber doctrine or incorporating cyber capabilities and operations into existing doctrine? Will the crafting of cyber foreign policy follow the pattern established by previous new technologies and domains, such as space?

2. Which countries' foreign policies or doctrines will shape the deployment of these technologies?

Which actors have the greatest ability to shape cyberspace? Historically, the U.S. has been the dominant actor. Will the character of cyberspace and cyber diplomacy change if, as Inkster (2016) posits, China replaces the U.S.? How can we measure these changes?

There is another line of inquiry that rests under the question of doctrine diffusion and the role of institutions and alliances. In what ways have alliances such as NATO, ANZUS, or U.S.-Japan been conduits for disseminating U.S. doctrine abroad? What role have these institutions, and others like them, played in shaping doctrine?

Estonia played a central role in Ukraine's response to Russian cyber intrusion. To what extent do neighboring states or particular sets of states serve as information sharing hubs for other states?

3. What can comparative studies add to the discussion?

We are in dire need of comparative studies outside of the dominant countries that occupy much of the scholarship. Ideally, our case studies would cover countries of varying geographic sizes and locations, levels of economic strength, military capabilities, industry characteristics, etc. In addition to work on the U.S. (e.g. Cavelty (2007), Segal (2013), and Gompert and Libicki (2014)), China (Inkster (2013), Segal (2013), Gompert and Libicki (2014), Lindsay et al. (2015), and Inkster (2016)), and Russia (Gvosdev (2012), Geers (2015), and Jaitner and Mattson (2015)), we hope to see a greater diversity of scholarship emerging on Australia, Brazil, France, Germany, Israel, Iran, Japan, New Zealand, North Korea, Singapore, South Africa, South Korea, and the U.K.

4. How do international organizations go about setting foreign policy and doctrine in this space? Or are they avoiding these types of decisions altogether?

We need more scholarship focusing on supranational and intergovernmental actors such as the United Nations, NATO, and the EU.

The Relationship Between State and Non-State Actors

Given the importance of non-state actors in cyberspace, there is a need for more work from within traditional international security as well as other fields. While the unit of interest in a great deal of security studies is the nation-state, there is robust literature on terrorism, organized crime, and other non-state actors.

In the 2016 report, surveyed work included two studies of non-state actors: Benson (2014) and Weinmann (2015).[27] Other notable works published prior to 2017 include Deibert (2003), Cavelty and Suter (2009), Applegate (2011), Healey (2011), Rattray and Healey (2011), Segal (2012), Fielder (2013), Bussolati (2015), Golden (2015), Tropina and Callanan (2015), and Borghard and Lonergan (2016).[28] Additional works published in this category in 2017 include Gross, Canetti, and Vashdi (2017), King et al. (2017), and Maurer (2017).[29] Papers and posters on this topic at ISA 2017 include Christensen.[30]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around state and non-state actors. We highlight three here:

1. What international security literatures that focus on non-state actors could be applied to this realm?

The many international security literatures that do not take the state as the dominant unit of analysis should be applied to cyber conflict. These include works on terrorism, intrastate conflict, organized crime, piracy, and public-private partnerships. There is also an extensive literature in international relations focused on corporations, non-governmental organizations, and regional and international institutions. This type of scholarship is present but sparse in the study of cyber conflict. For example, Benson (2014), Gabriel (2015), and Gross, Canetti, and Vashdi (2017) have published work examining cyberterrorism. Applegate (2011) and Segal (2012) focused on the emergence of cyber militias. Tropina and Callanan (2015) focused on the Internet industry's role in cybersecurity and crime, and Golden (2015) focused on the creation of new private-public partnerships. Most recently, King (2017) focused on social media and information campaigns. Future work drawing on these literatures and delineating how cyber conflict diverges from existing models would help to close the non-state scholarship gap in the emerging field.

2. What is the importance of proxy actors? What are the characteristics of relationships between states and non-state actors?

Our discussion referenced two types of relationships: non-state actors as proxies for states and public-private partnerships. Scholarship is emerging on both: works by Borghard and Lonergan (2016) and Maurer (2017) examine proxy actors and mercenaries in cyberspace, while works by Cavelty and Suter (2009), Golden (2015), and Tropina and Callanan (2015) examine public-private partnerships. Can we create a more general typology of relationships between state and non-state actors? What types of relationships exist beyond public-private partnerships, proxies, militias, and mercenaries? What types of case studies would be useful for illuminating these relationships and their strategic consequences?

3. Can non-state actors can be both victims and perpetrators in cyber conflict.

Non-state actors such as proxies, militias, terrorist groups, and individuals can be perpetrators of cyber-attacks. Yet non-state actors such as infrastructure or utility providers, private companies, and individuals can also be the victims of these attacks. Other non-state actors provide tactical support and are neither perpetrator nor victim but rather quasi-first responders. Take Computer Emergency Readiness Teams (CERTs) as an example. What types of relationships exist between states and non-state actors with different connections to cyber conflict?

In conclusion, in order to fully grapple with the role non-state actors play in cyber conflict, we must first classify those actors by type, the characteristics of their relationships with each other and with states, and the role they play in conflicts.

Norms and Norm Diffusion

The discussion of norms and norm diffusion was relatively developed compared to many of the other subtopics presented in this White Paper. While the Copenhagen School has taken the lead on researching the securitization of cybersecurity, there remain many topics of interest to scholars and practitioners. These questions include: How do states promote norms in cyberspace, and when do they accept them? Do existing norms apply, or will new ones be developed? What norms are emerging? Does just war theory apply? How are non-state actors engaged in norm entrepreneurship?

In the 2016 report, surveyed work included Nissenbaum (2005), Hansen and Nissenbaum (2009), Maurer (2011), Cavelty (2015), Grigsby (2015), and Mazanec (2015).[31] Other notable works published prior to 2017 include Finnemore (2011), Tikk (2011), Yannakogeorgos (2011), Stevens (2012), Hurwitz (2014), Farrell (2015), Erskine and Carr (2016), and Osula and Rõigas (2016).[32] Additional works published within the last year include Farrell and Glaser (2017).[33] Papers and posters on this topic at ISA 2017 include Barrett and Shamai and Mazanaec.[34]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around norms and norm diffusion. We highlight four here:

1. Can we begin to determine norms in cyberspace?

Do we have examples of norms and norm formation around cyber conflict? Are there issues that certain actors are championing as norms but that have yet to rise to the standard of a norm? Have any taboos been established? In what areas, such as state-sponsored espionage, have international norms simply not been significantly pursued or developed yet? n Across all of these questions one question stands out, how can we prove the existence of a norm? Are apparent examples of self-restraint around certain norms enough?

Identifying norms in cyberspace is particularly challenging. Erskine and Carr (2016) point to three complicating factors. First, cyberspace is a domain in which practices and the technology they stem from are both new and rapidly changing. Second, there are persisting, competing value systems that create additional tension for and differing perceptions of cybersecurity. Third, while norms set guidelines and expectations for behavior by specific actors, cyberspace involves a wide range of potential actors, and it can be unclear to which actor (or moral agent) a norm might apply.

With these limitations in mind, much of the discussion here remains prescriptive (what norms we would like to see developed) or theoretical (how cyber norms might emerge and why). Tikk (2011), for example, argues that four sources of law—soft, organizational, national and international agreements, and customary law—are necessary for cyber security. In contrast, Finnemore (2011) applies lessons from the emergence of international norms in the past to predict patterns for diffusion, contestation, modification, and acceptance of potential cyber norms. In a departure from largely theoretical and/or prescriptive work, Yannakogeorgos (2011) conducted an empirical examination of an existing cyber norm by tracing the development of ICANN Internet governance over the past decade.

Significant attention has also been paid to the application of legal norms and agreements around conflict and warfare to the cyber domain. This topic is covered in more detail in the Law White Paper in this series.

2. What factors are driving norm creation?

If specific norms are in fact emerging, what factors are driving them? Is it concerns around destabilization or escalation? Are they then emerging from a general consensus that cyber conflict without norms would be dominated by undesirable characteristics? Or perhaps these norms are driven by states with limited resources and significant external threats. Perhaps, as Farrell and Glaser (2017) argue, norms in U.S. doctrine are created in response to effects rather than means. Cyber weapons, then, only require a new set of norms if their effects diverge from those for which norms already exist.

In this process, are norms (or potential norms) from different domains or communities competing? Do norms from business communities crash into norms from departments of defense? Are some states advocating for particular norms but encountering resistance from others? Where, by contrast with the points of convergence discussed above, are the points of tension?

3. What role are non-state actors playing in establishing norms?

Given that non-state actors play a much more central role in this security space than in others before it, how are they shaping norm formation? Which types of actors are taking the lead? What are their interests? Take Microsoft's efforts to establish a digital Geneva Convention as just one possible example.

International Institutions and Cooperation

This category is a broad catch-all for many different forms of cooperation, such as military alliances, governance, regime creation, and international institutions. Given the lack of depth and breadth in studies emerging so far, somewhat disparate works found themselves grouped into this single bucket. During the panel discussion, this category was pointed to as a rich area for future research. Interestingly, a large number of the papers and posters presented at ISA 2017 were on these topics.

While a broad international institutions and cooperation category was not part of the 2016 report, highlighted work focusing on a subset of cooperation —"Cyber Arms Control Institutions and Regimes"—included Dipert (2010), Geers (2010), Knake (2010), Lin (2012), Schmitt (2013), and Valeriano and Maness (2014).[35] Other notable works published prior to 2017 in the broader cooperation and international institutions literature include Axelrod (2010), Hathaway (2010), Hunker (2010), Tikk (2010), Healey and Bochoven (2011), Hurowitz (2012), Forsyth (2013), Goldsmith (2013), Clark et al. (2014), DeNardis (2014), and Shackelford and Craig (2014).[36] Additional work published in 2017 includes Lindsay (2017) and Rovner and Moore (2017).[37] Papers and posters on this topic at ISA 2017 included An, Brandao and Camisao, Coleman, Diersch, Griffith, and Yoo.[38]

Several central questions emerged from our preparatory materials and the subsequent panel discussion around international institutions and cooperation. We highlight one here:

1. What about international security literatures that focus on cooperation?

Within international security, numerous literatures focus on cooperation in the face of security threats. Pulling these literatures into discussions around cyberspace would fill a clear and significant gap in existing scholarship. Early efforts in this regard remain sporadic and nascent.

Of note is emerging scholarship testing mechanisms identified as driving security cooperation more broadly within the context of cyberspace. For example, Rovner and Moore (2017) investigate whether hegemonic stability theory applies to cyberspace, specifically whether hegemonic leadership on the part of the U.S. ameliorates collective action problems in cyberspace. Forsyth (2013) also looked at the role of great powers. Ultimately, he argued, in contrast to Hurwitz's (2012) view, that great powers have provided existing structures for cyberspace. In other words, "cyberspace is what great powers make of it."

In addition, the literatures on alliance formation, evolution, and termination can be applied to questions on the utility of certain types of alliances for cyber conflict, whether existing alliances will be utilized, and how alliances will evolve given this new threat. Griffith's 2017 ISA paper on alliance theory sought to draw attention to the utility of these theories by examining U.S. alliances. By specifically addressing the utility of alliance theory, this work builds on previous research regarding the role of military alliances in cyber-defense, which had largely taken two forms: (1) empirical, as in Healey and Bochoven's 2011 work, examining how existing alliances have responded to potential cyber conflicts, and (2) prescriptive, as in works by Hathaway (2010), Hunker (2010), and Tikk (2010), asking how existing alliances should respond to the changing threat environment.

Similarly, arms control literature can be drawn upon to examine cyber arms control and its limitations. Geers (2010) and Lin (2012) provide a useful starting place here.

Two broader fields of study or literatures that extend beyond security cooperation are also worth mentioning here. First, literatures focusing on international law can be and have been applied to cyber conflict. The *Tallinn Manuals* (see Schmitt (2013)) represent a significant effort in this regard. Law and legal cooperation is discussed in greater detail in the White Paper on the legal and ethical issues embedded within the study of cyber conflict. Second, questions around the governance of cyberspace likewise span multiple White Papers, touching upon issues ranging from legal to economic concerns and from operational to strategic dynamics. Out of all the cooperative efforts examined so far, governance has received a significant amount of attention. Take, for example, Axelrod (2010), Clark et al. (2014), and Shackelford and Craif (2014), as well as the ongoing debate between multilateral (state and public agency led) and multi-stakeholder (public-private partnership) governance models.

In conclusion, international security cooperation remained one of the core gaps identified in our preparation for the panel and in the subsequent panel discussion. One possible first step for future work is to examine the applicability of existing theories of security cooperation to cyberspace. As that work is completed, we hope to see this category break apart into several distinct sub-literatures.

Panel and Plenary Discussions

During the panel discussion directly following our presentation of the state of the field on this topic, audience members raised several questions that did not easily fit into the buckets above. The following is an overview of four central questions for your reference.

1. In what ways does cyberspace affect other security interests?

We should also be looking at how cyberspace affects other outcomes of interest, such as nuclear stability. In addition, we should ask how cyber tools affect the broader outcome of interest in each literature, such as balance of power, cooperation, stability, escalation, etc. How do cyber tools alter, for example, the overall offense-defense balance at a strategic level?

2. Where do psychological and information warfare fit?

This question was raised in the 2016 panel and again in 2017 with more vigor, given the recent Russian information operations during the U.S. and French elections. Psychological warfare requires more study both as an independent form of warfare and as a domain where cyber tools play a role.

3. How should we approach potential drivers of change? Should we expect all or some of the dynamics that define cyber conflict today to persist in the future?

As a field, we need to be conducting future-oriented research rather than assuming that the dynamics we observe today will persist. How might the strategic dynamics of conflict be different in five years? In ten years? In twenty years? What new technologies (e.g., artificial intelligence) might drive that change?

4. How can we integrate economic concerns into cyber conflict and cyber security?

Our adversaries are attempting to use economic means to hurt us and help themselves. This plays into the broader strategic concerns of any given country. What are the boundaries between economic and security concerns? Is there agreement on these boundaries?

Summary and Recommendations

The purpose of this White Paper was threefold: (1) to capture the evolution of the field since the 2016 State of the Field Conference, (2) to provide an overview of the existing scholarship focusing on the strategic dynamics of cyberspace, and (3) to identify where more rigorous research could expand the frontiers of the field.

The paper also highlighted four takeaways. First, there is a persisting tension between academics and policy practitioners regarding the utility of international security to the study of cyber conflict. Second, the topics the field has chosen to study remained largely consistent between the 2016 conference and the 2017 conference. Deterrence remains over-researched, while domestic politics remains severely underdeveloped. International cooperation saw the most attention in the form of ISA papers. Empirical work and case studies are focused on a handful of countries. Third, the conceptual boundaries between tactical, operational, and strategic dynamics in cyberspace are difficult to maintain, but still lead to useful research. Fourth, as a field, we need to pay attention to both the destructive outcomes of cyber conflict and the motivating strategic goals and outcomes for which cyber tools are being mobilized. These are two separate intellectual inquiries and should be clearly distinguished from one another.

It is also important to note that there remain some key limitations to the design of this panel and subsequent White Paper. First, some important new works may be missing from this overview. We hope to continue to expand the scope of the work represented and encourage readers to point us to work, new and old, that we may have missed. Second, no single discipline will be able to comprehensively address the realities of cyber conflict. International security, as highlighted in this White Paper, maintains broad utility around certain sets of questions, while other fields of inquiry will provide additional insight into others. Moreover, while it is important to make reference to the international security sub-literatures explored here, it will also be productive to show the ways in which some of these theories and models hold limited or incorrect explanatory power in this new threat space. That said, many of these models continue to hold significant utility and should not simply be discarded on the assumption that "everything has changed." Third, this overview of the state of the field is centered around an academic political science audience. The questions policy practitioners are asking likely have some overlap with those discussed but also branch out into different interests, which are not captured here.

With these limitations in mind, we hope that this White Paper proves useful as both a starting place for new entrants into this field and a reference for those already enmeshed in these debates. To echo Maness and Segal's 2016 report, scholars need to continue to be "theoretically innovative and empirically grounded" to move the field forward. During the 2018 State of the Field Conference, we hope to see many of the questions outlined above answered, as well as new efforts to fill those gaps that persist.

About the Authors

Melissa K. Griffith is a Ph.D. Candidate in Political Science at the University of California, Berkeley.

Adam Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations.

End Notes

[1] The 2017 Conference was the second State of the Field of Cyber Conflict meeting. The event was co-hosted by the Cyber Conflict Studies Association and the Saltzman Institute of War and Peace Studies at Columbia University's School of International and Public Affairs (SIPA). For an overview of the conference, refer to www.cyberconflict.org/blog/2017/6/23/state-of-the-field-of-cyber-conflict-workshop-june-2017.html

[2] To review Maness and Segal's 2016 State of the Field assessment, refer to SIPA's "Cyber Conflict State of the Field Workshop Report": http://static1.1.sqspcdn.com/static/f/956646/27604316/1498262610577/SOTF_Review_Copy.pdf?token=OROvr5%2FKs5iuP2UX8tX6Cv-J%2FI0U%3D

[3] Griffith, Melissa K. and Trey Herr. 2017. "Is the Strategic Corporal on Your Twitter Feed?" in *Net Politics* and *Digital and Cyberspace Policy Program* from the Council on Foreign Relations: July 12. www.cfr.org/blog/strategic-corporal-your-twitter-feed

[4] For examples of work on the RMA, which falls largely outside the scope of this specific review of literature, refer to Metz, Steven and James Kievit. 1994. "The Revolution in Military Affairs and Conflict Short of War." *United States Army War College Strategic Studies Institute*; Blank, Stephen J. 1996. "Preparing for the Next War." *Strategic Review* 24(2): 17–25; Biddle, Stephen. 1996. "Victory Misunderstood: What the Gulf War Tells Us About the Future of Conflict." *International Security* 21(2): 139–179; Cohen, Eliot A. 1996. "A Revolution in Warfare." *Foreign Affairs*; Davis, Norman C. 1996. "An Information-Based Revolution in Military Affairs." *Strategic Review* 24(1): 43–53; Friedman, George and Meredith Friedman. 1998. *The Future of War: Power, Technology and American World Dominance in the Twenty-first Century* (St. Martin's Griffin Publishers); Gongora, Thierry and Harald Von Riekhoff. 2000. *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century* (Greenwood Press); Andréani, Gilles, Christoph Bertram, and Charles Grant. 2001. *Europe's Military Revolution* (Center for European Reform); and Sloan, Elinor C. 2002. *The Revolution in Military Affairs*. 1st 3dition (McGill-Queen's University Press).

[5] Lindsay, Jon R. and Lucas Kello. 2014. "Correspondence: A Cyber Disagreement." *International Security* 39(2): 181–192.

[6] Arquilla, John and David Ronfeldt. 1993. "Cyberwar Is Coming!" Comparative Strategy 12(2): 141–65. doi:10.1080/01495939308402915; Clarke, Richard A. and Robert Knake. 2011. *Cyber War: The Next Threat to National Security and What to Do About It.* Reprint edition (Ecco); Choucri, Nazli. 2012. *Cyberpolitics in International Relations* (MIT Press); Junio, Timothy. 2013. "A Theory of Information Warfare." University of Pennsylvania dissertation; Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38(2): 7–40; Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10(1): 86–103. doi:10.1080/19331681.2012.759059; Rid, Thomas. 2013. *Cyber War Will Not Take Place* (Hurst & Company); and Lindsay, Jon R. and Lucas Kello. 2014. "Correspondence: A Cyber Disagreement." *International Security* 39(2): 181–92. doi:10.1162/ISEC_c_00169.

[7] Kello, Lucas. 2017. *The Virtual Weapon and International Order*. Kindle edition (Yale University Press); Lindsay, Jon Randal. 2017. "Restrained by Design: The Political Economy of Cybersecurity." *Digital Policy, Regulation and Governance* 19(6); Perkovich, George and Ariel E. Levite, eds. 2017. *Understanding Cyber Conflict: Fourteen Analogies* (Georgetown University Press).

[8] For one such example, refer to Mulligan, Deirdre K. and Fred B. Schneider. 2011. "Doctrine for Cybersecurity." *Daedalus* 140(4): 70–92, who apply the provision of public health as a public good to cybersecurity provisions.

9. Kugler, Richard L. 2009. “‘Deterrence of Cyber Attacks.’” In *Cyberpower and National Security*, Franklin Kramer, Stuart H. Starr, and Larry K. Wentz, eds. 1st edition (Potomac Books): 309–42; Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar* (RAND). www.books24x7.com/marc.asp?bookid=54204; Goodman, Will. 2010. “Cyber Deterrence: Tougher in Theory than in Practice?” *U.S. Senate Washington, DC Committee on Armed Services* 4(3). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA528033; National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (The National Academies Press); Nye, Joseph S. 2011. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* 5(4): 18–38; Cooper, Jeffrey. 2012. “A New Framework for Cyber Deterrence.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Derek S. Reveron, ed. (Georgetown University Press): 105–120. www.jstor.org/stable/j.ctt2tt6rz; Valeriano, Brandon and Ryan C. Maness. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research* 51(3): 347–60. doi:10.1177/0022343313518940; and Gartzke, Erik and Jon R. Lindsay. 2015. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24(2): 316–48. doi:10.1080/09636412.2015.1038188.

10. Harknett, Richard J. 1996. “Information Warfare and Deterrence.” *Parameters*: 93–107; Clark, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins); Liff, Adam P. 2012. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35(3): 401–428; Tsagourias, Nicholas. 2012. “Cyber Attacks, Self-Defence and the Problem of Attribution.” *Journal of Conflict and Security Law* 17(2): 229–44; Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38(2): 41–73; Iasiello, Emilio. 2013. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7(1): 54–67; Schmitt, Michael N. and Liis Vihul. 2014. “Proxy Wars in Cyberspace: The Evolving International Law of Attribution.” *Fletcher Security Review* 1(2): 54–73; Lindsay, Jon R. 2015. “Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack.” *Journal of Cybersecurity* 1(1): 53–67; Healey, Jason. 2016. “Beyond Attribution: Seeking National Responsibility in Cyberspace.” *Atlantic Council*; and Lupovici, Amir. 2016. “The ‘Attribution Problem’ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step Forward.” *International Studies Perspectives*.

11. Borghard, Erica D and Shawn W. Lonergan. 2017. “The Logic of Coercion in Cyberspace.” *Security Studies* 26(3): 452–481; Chen, Jim. 2017. “Deterrence and its Implementation in Cyber Warfare.” In *ICCWS 2017-Proceedings of the 12th International Conference on Cyber Warfare and Security* (ACPIL); Davis II, Jon S., Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND); Edwards, Benjamin, Alexander Furnas, Stephanie Forrest and Robert Axelrod. 2017. “Strategic Aspects of Cyberattack, Attribution, and Blame.” *Proceedings of the National Academy of Sciences of the United States of America* 114(11): 2825–2830; Fischerkeller, Michael. 2017. “Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies.” *Survival: Global Politics and Strategy* 59(1): 103–134; Harknett, Richard J. and Michael P. Fischerkeller. 2017. “Deterrence is Not a Credible Strategy for Cyberspace.” *Orbis* 61(3); Harknett, Richard R. and Joseph Nye Jr. 2017. “Is Deterrence Possible in Cyberspace?” *International Security* 42(2): 196–199; Mandel, Robert. 2017. *Optimizing Cyber Deterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks* (Georgetown University Press); Nye, Joseph. 2017. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41(3): 44–71; Sharp, Travis. 2017. “Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony.” *Journal of Strategic Studies* 40(7): 898–926.

12. ISA 2017: Cunningham, Fiona (MIT). “Seizing the Initiative or Controlling Escalation? China’s Changing Approach to Cyber Deterrence”; Lupovici, Amir (Tel Aviv University). “Israel and the (Social) Construction of Cyber Deterrence”; and Wilner, Alex (Carleton University). “State and Non-State Cyber Deterrence: Bridging IR by Crossing Disciplines.”

13. Healey, Jason. 2016. “The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities.” Submitted to *The Journal of Cybersecurity*: www.americanbar.org/content/dam/aba/administrative/law_national_security/Jason%20Healey%20The%20Cartwright%20Conjecture.authcheckdam.pdf

14. See, e.g., Fearon, James. 1998. “Bargaining, Enforcement, and International Cooperation.” *International Organization* 52 (Spring): 269–305.

15. Andres, Richard. 2012. “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*, Derek S. Reveron, ed. (Georgetown University Press). www.jstor.org/stable/j.ctt2tt6rz.; Liff, Adam P. 2012. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35(3): 401–28. doi:10.1080/01402390.2012.663252; Fielder, James D. 2013. “Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion.” *Small Wars Journal* 9(6). http://smallwarsjournal.com/jrnl/art/bandwidth-cascades-escalation-and-pathogen-models-for-cyber-conflict-diffusion; Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38(2): 41–73. doi:10.1162/ISEC_a_00136; Peterson, Dale. 2013. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies* 36(1): 120–24. doi:10.1080/01402390.2012.742014; Saltzman, Ilai. 2013. “Cyber Posturing and the Offense-Defense Balance.” *Contemporary Security Policy* 34(1): 40–63. doi:10.1080/13523260.2013.771031; Rid, Thomas and Ben Buchanan. 2015. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38(1–2): 4–37. doi:10.1080/01402390.2014.977382; Valeriano, Brandon and

Ryan C. Maness. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research* 51(3): 347–60. doi:10.1177/0022343313518940; and Gartzke, Erik and Jon R. Lindsay. 2015. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24(2): 316–48. doi:10.1080/09636412.2015.1038188.

16. Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press); Lin, Herbert. 2010. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* 4(63): 63–86; Lin, Herbert. 2012. “Escalation Dynamics and Conflict Termination in Cyberspace.” *Strategic Studies Quarterly* 6(3): 46–70; Malone, Patrick J. 2012. “Offense-Defense Balance in Cyberspace: A Proposed Model.” *Naval Postgraduate School*; Fielder, James D. 2013. “Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion.” *Small Wars Journal* 9(6); Kello, Lucas. 2013. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38(2): 7–40; Lieber, Keir. 2013. “The Offense-Defense Balance and Cyber Warfare.” In Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Naval Postgraduate School); Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22(3): 365–404; Rid, Thomas. 2013. *Cyber War Will Not Take Place* (Oxford University Press); and Harknett, Richard and Emily Goldman. 2016. “The Search for Cyber Fundamentals.” *Journal of Information Warfare* 15(2): 81–88.

17. Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford University Press); Slayton, Rebecca. 2017. “What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” *International Security* 41(3): 72–109; and Smeets, Max. 2017. “A Matter of Time: On the Transitory Nature of Cyberweapons.” *Journal of Strategic Studies* 41(1–2).

18. ISA 2017: Buchanan, Ben (Harvard University). “The Cybersecurity Dilemma”; Loleski, Steven (University of Toronto). “Exploit It All: Threats, Vulnerabilities, and the Cyber Security Dilemma”; Monte, Matthew (Self). “Offense-Defense Asymmetries: A View from Inside Cyber Operations”; Slayton, Rebecca M. (Cornell University). “Reframing the Cyber Offense-Defense Balance: From Technology to Skilled Practice.”

19. Smith III, Frank L. 2017. “Quantum Technologies and International Security.” CLTC Visiting Scholar Paper Workshop, UC, Berkeley.

20. Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace* (MIT Press); Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. 1st edition (Cambridge University Press); Kramer, Franklin, ed. 2009. *Cyberpower and National Security*. 1st edition (Potomac Books); Nye, Joseph S. 2010. “Cyber Power.” Essay from the Belfer Center for Science and International Affairs, Harvard Kennedy School: http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html; Betz, David J. and Tim Stevens. 2012. *Cyberspace and the State: Towards a Strategy for Cyber-Power*. 1st edition (Routledge); Rid, Thomas and Peter McBurney. 2012. “Cyber-Weapons.” *The RUSI Journal* 157(1): 6–13. doi:10.1080/03071847.2012.664354; Sheldon, John B. 2012. “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*, Derek S. Reveron, ed. (Georgetown University Press): 207–224; Healey, Jason, ed. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association); Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22(3): 365–404. doi:10.1080/09636412.2013.816122; and Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. 1st edition (Public Affairs).

21. Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. 2010. *Cyberpower and National Security* (National Defense University Press and Potomac Books); Klimburg, Alexander. 2011. “Mobilizing Cyber Power.” *Survival* 53(1): 41–60; Betz, David. 2012. “Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed.” *Journal of Strategic Studies* 35(5): 689–711; Ebert, Hannes, and Tim Maurer. 2013. “Contested Cyberspace and Rising Powers.” *Third World Quarterly* 34(6): 1054–1074; Sheldon, John B. 2014. “Geopolitics and Cyber Power: Why Geography Still Matters.” *The Journal of the National Committee on American Foreign Policy* 36(5): 286–293.

22. Borghard, Erica D. and Shawn Lonergan. 2017. “The Logic of Coercion in Cyberspace.” *Security Studies* 26(3); Kello, Lucas. 2017. *The Virtual Weapon and International Order*. Kindle edition (Yale University Press); Maurer, Tim. 2017. *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press); and Sharp, Travis. 2017. “Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony.” *Journal of Strategic Studies*.

23. ISA 2017: Langø, Hans-Inge (University of Texas at Austin). “Mutually Assured Vulnerability: An Ecological Approach to the Study of Coercion and Power in Cyberspace”; and Maness, Ryan (Northeastern University). “Cyber Compellence: Applying Coercion in the Information.”

24. Cavelty, Myriam Dunn. 2007. *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age* (Routledge). www.tandfebooks.com/isbn/9780203937419; Gvosdev, Nikolas K. 2012. “The Bear Goes Digital: Russia and its Cyber Capabilities.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Derek Reveron, ed. (Georgetown University Press). www.jstor.org/stable/j.ctt2tt6rz; Reveron, Derek S., ed. 2012. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Georgetown University Press); Guitton, Clement. 2013. “Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?” *European Security* 22(1): 21–35. doi:10.1080/09662839.2012.749864; Inkster, Nigel. 2013. “Chinese Intelligence in the Cyber Age.” *Survival: Global Politics and Strategy* 55(1): 45–66. doi:10.1080/00396338.2013.767405; Inkster, Nigel. 2016. *China’s Cyber Power* (The International Institute for Strategic Studies); Junio, Timothy. 2013. “A Theory of Information Warfare.” University of Pennsylvania dissertation; Segal, Adam. 2013. “The code not taken: China, the United States, and the future of cyber espionage.” *Bulletin of the Atomic Scientists*, 69(5), 38–45; Axelrod, R. and R. Iliev. 2014. “Timing of Cyber Conflict.” Proceedings of the National Academy of Sciences 111(4): 1298–1303.

doi:10.1073/pnas.1322638111; Gompert, David C. and Martin Libicki. 2014. “Cyber Warfare and Sino-American Crisis Instability.” *Survival* 56(4): 7–22. doi:10.1080/00396338.2014.941543; Lindsay, John. R. 2014. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39(3): 7–47; Geers, Kenneth. 2015. *Cyber War in Perspective: Russian Aggression against Ukraine* (CCDCOE). http://scholar.google.com/scholar?cluster=9137378561972954249&hl=en&oi=scholarr; Jaitner, Margarita and Peter A. Mattsson. 2015. “Russian Information Warfare of 2014.” In *Cyber Conflict: 2015 Conference on Architectures in Cyberspace* (IEEE): 39–52. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7158467; Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. 1st edition (Oxford University Press); Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War* (Simon & Schuster); and Maness, Ryan C. and Brandon Valeriano. 2016. “The Impact of Cyber Conflict on International Interactions.” *Armed Forces & Society* 42(2): 301–23. doi:10.1177/0095327X15572997.

25. Inkster, Nigel. 2016. *China’s Cyber Power* (IISS).

26. ISA 2017: Barrinha, Andre Filipe (Canterbury Christ Church University and Centre for Social Studies) and Thomas Renard (Egmont, Brussels). “Cyber-diplomacy and Change in World Politics.”

27. Benson, David C. 2014. “Why the Internet is not Increasing Terrorism.” *Security Studies* 23(2): 293–328. doi: 10.1080/09636412.2014.905353; and Weimann, Gabriel. 2015. *Terrorism in Cyberspace: The Next Generation* (Columbia University Press).

28. Deibert, Ronald J. 2003. “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace.” *Millennium: Journal of International Studies* 32(3); Cavelty, Myriam Dunn and Manuel Suter. 2009. “Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection.” *International Journal of Critical Infrastructure Protection* 2(4): 179–187; Applegate, Scott D. 2011. “Cybermilitias and Political Hackers—Use of Irregular Forces in Cyberwarfare.” *IEEE Security and Privacy Magazine* 9(5): 16–22; Healey, Jason. 2011. “The Spectrum of National Responsibility for Cyberattacks.” *Brown Journal of World Affairs* 18(1): 57–69; Rattray, Gregory and Jason Healey. 2011. “Chapter 5: Non-State Actors and Cyber Conflict.” In *America’s Cyber Future: Security and Prosperity in the Information Age*, Kristin M. Lord and Travis Sharp, eds. (CNAS): 67–83; Segal, Adam. 2012. “The Rise of Asia’s Cyber Militias.” *The Atlantic*: www.theatlantic.com/international/archive/2012/02/the-rise-of-asias-cyber-militias/253487/; Fielder, James D. 2013. “Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion.” *Small Wars Journal* 9(6); Bussolati, Nicolò. 2015. “The Rise of Non-State Actors in Cyberwarfare.” In *Cyber War: Law and Ethics for Virtual Conflicts*, Jens David Ohlin, Kevin Govern, and Claire Finkelstein, eds. (Oxford Scholarship Online); Golden, Chris. 2015. “Creating New Private-Public Partnerships in Cybersecurity.” *National Cybersecurity Institute Journal* 2(3); Tropina, Tatiana and Cormac Callanan. 2015. “Self- and Co-regulation in Cybercrime, Cybersecurity and National Security” (SpringerBriefs in Cybersecurity); and Borghard, Erica D. and Shawn W. Lonergan. 2016. “Can States Calculate the Risks of Using Cyber Proxies?” *Orbis* 60(3): 395–416.

29. Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 2017. “Cyberterrorism: Its Effects on Psychological Well-being, Public Confidence and Political Attitudes.” *Journal of Cybersecurity* 3(1); King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument.” *American Political Science Review* 111(3): 484–501; Maurer, Tim. 2017. *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press).

30. ISA 2017: Christensen, Kristoffer (University of Copenhagen). “‘It Is Not Even There’: Topologies of Cyber Security in the Practice of Private Companies.”

31. Nissenbaum, Helen. 2005. “Where Computer Security Meets National Security.” *Ethics and Information Technology* 7(2): 61–73. doi:10.1007/s10676-005-4582-3; Hansen, Lene and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53(4): 1155–75. doi:10.1111/j.1468-2478.2009.00572.x; Maurer, Tim. 2011. “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. http://belfercenter.ksg.harvard.edu/publication/21445/cyber_norm_emergence_at_the_united_nationsan_analysis_of_the_uns_activities_regarding_cybersecurity.html; Cavelty, Myriam Dunn. 2007. “The Normalization of Cyber-International Relations.” In *Strategic Trends* 2015, Oliver Thränert and Martin Zapfe, eds. (Center for Security Studies): 81–98. www.researchgate.net/publication/274076687_The_Normalization_of_Cyber-International_Relations; Grigsby, Alex. 2015. “The UN GGE on Cybersecurity: What is the UN’s Role?” *Council on Foreign Relations—Net Politics* (April) http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/; and Mazanec, Brian M. 2015. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (University of Nebraska Press).

32. Finnemore, Martha. 2011. “Cultivating International Cyber Norms.” In *America’s Cyber Future: Security and Prosperity in the Information Age*, Kristin M. Lord and Travis Sharp, eds. (CNAS); Tikk, Eneken. 2011. “Ten Rules for Cyber Security” *Survival* 53(3): 119–132; Yannakogeorgos, Panayotis. 2011. “Cyberspace, the New Frontier – and the Same Old Multilateralism.” In *Global Norms, American Sponsorship and the Emerging Patterns of World Politics*, S. Reich, ed. (Palgrave); Stevens, Tim. 2012. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace.” *Contemporary Security Policy* 33(1):148–70; Hurwitz, Robert. 2014. “The Play of States: Norms and Security in Cyberspace.” *American Foreign Policy Interests* 36(5); Farrell, Harry. 2015. “Promoting Norms for Cyberspace.” *Council on Foreign Relations*; Erskine, Toni and Madeline Carr. 2016. “Beyond ‘Quasi-Norms’: The Challenges and Potential of Engaging with Norms in Cyberspace.” In *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO Cooperative

Cyber Defence Centre of Excellence); and Osula, Anna-Maria and Henry Rõigas, eds. 2016. *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO Cooperative Cyber Defence Centre of Excellence).

33. Farrell, Henry and Charles L. Glaser. 2017. "The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine." *Journal of Cybersecurity* 3(1).

34. ISA 2017: Barrett, Edward T. (U.S. Naval Academy). "Reliable Old Wineskins: The Applicability of the Just War Tradition to Military Cyber Operations"; and Shamai, Patricia (University of Portsmouth) and Brian M. Mazanaec (George Mason University). "Stigmatizing Cyber War: Mission Impossible?"

35. Dipert, Randall R. 2010. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9(4): 384–410; Geers, Kenneth. 2010. "Cyber Weapons Convention." *Computer Law & Security Review* 26(5): 547–551; Knake, Robert K. 2010. *Internet Governance in an Age of Cyber Insecurity*. Council Special Report, no. 56 (Council on Foreign Relations); Lin, Herbert S. 2012. "Arms Control in Cyberspace: Challenges and Opportunities." *World Politics Review* (March); Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press); and Valeriano, Brandon and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011." *Journal of Peace Research* 51(3): 347–60. doi:10.1177/0022343313518940.

36. Axelrod, Robert. 2010. "Beyond the Tragedy of the Commons: A Discussion of *Governing the Commons*." *Perspectives on Politics* 8(2): 580–82; Hathaway, Melissa E. 2010. "Toward a Closer Digital Alliance." *SAIS Review of International Affairs* 30(2); Hunker, Jeffrey. 2010. "Cyber War and Cyber Power: Issues for NATO Doctrine." *NATO Defense College, Rome*, 62; Tikk, Eneken. 2010. "Global Cybersecurity–Thinking About the Niche for NATO." *SAIS Review of International Affairs* 30(2); Healey, Jason and Leendert van Bochoven. 2011. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow." Issue Brief for *The Atlantic Council*; Hurwitz, Roger. 2012. "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly* 6(3); Forsyth, James W. 2013. "What Great Powers Make of It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly* 7(1); Goldsmith, Jack. 2013."Cybersecurity Treaties: A Skeptical View." Hoover Institution; Clark, David, Thomas Berson, and Herbert S. Lin, eds. 2014. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (National Academies Press); DeNardis, Laura. 2014. *The Global War for Internet Governance* (Yale University Press); and Shackelford, Scott and Amanda Craig. 2014. "Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Ω*(5)0.

37. Lindsay, Jon R. 2017. "Restrained by Design: The Political Economy of Cybersecurity." Digital Policy, Regulation, and Governance 19(6); and Rovner, Joshua and Tyler Moore. 2017. "Does the Internet Need a Hegemon?" Journal of Global Security Studies 2(3): 184–203.

38. ISA 2017: An, Jungbae (Yonsei University). "A Handful of Technocrats or Supranational Policy Network: Technical Community in Global Internet Governance"; Brandao, Ana Paula (CICP, University of Minho) and Isabel Camisao (CICP, University of Coimbra). "Framing the Cybersecurity Agenda: An Analysis of the Commission's Entrepreneurship"; Coleman, Liv (University of Tampa). "Pressure on Defense: Cybersecurity and the U.S.-Japan Alliance"; Diersch, Verena (University of Cologne). "Cyberspace as a Realm for Intelligence Cooperation – Is Technology the Driving Factor?"; Griffith, Melissa K. (UC, Berkeley). "The Durability of an Alliance: NATO and Cyber-Defense"; and Yoo, In Tae (Yonsei University). "New Wine into Old Wineskins? Regime Diffusion in Cyberspace through International Trade."

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

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

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