CCSA
Cyber Conflict Studies Association

Economic Dimensions of Cyber Conflict

AUTHORS: Dr. Chris Demchak and Benjamin Schechter
SERIES EDITOR: Justin Key Canfil

Introduction

As the relevance and academic interest in cyber conflict studies deepen and the methods and theory applied to the subject matter multiply, it is evitable that the relevance of cybersecurity studies to other academic areas should also expand. The increasing linkages between cyber conflict studies and other established disciplines mirror cyber's deepening integration in diverse areas ranging from communications and finance to healthcare. The rise of highly insecure and highly interconnected globe-spanning digital networks has not only affected existing systems like finance but also radically redefine them. The question is raised whether cyber's impacts force modifications into existing theory and thought across other academic areas, or perhaps even radical reassessments. More to the point of this report, while cyber-driven interconnectedness spreads, so do the threats that accompany the use of cyber. These threats present serious, unanswered quandaries for some academic disciplines, such as economics.

This year was the first State of the Field to feature the Economic Impact of Cyber Threats panel. The panel explored how cyber insecurity impacts economies at the firm and state level, and how that may have implications for existing economic theory. The panel discussions investigated how existing economic theory does, or does not, account for increasingly severe cyber threats and systemic cyber vulnerability. This panel was intended to mark the beginning of an ongoing discussion, laying a groundwork for more substantive work.

Discussions touched on a host of topics, related to the effects of a highly integrated world, deeply reliant on cyberinfrastructure. There was a consensus among discussants that the impacts of cyber threats on national and international economics were consequential and had security implications. Furthermore, there was a general consensus that this problem set had received insufficient scrutiny and study by established scholars. The discussion had a number of relevant takeaways. As was expected, there is still pushback on whether the degree to which this research is necessary or if the problem is being framed is correct. Is it a fundamental issue at the theoretical level or if it is evidence of insufficient application of existing theory to the problem. Issues of how to effectively conduct the research and

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.

how to make this line of inquiry relevant and viable for scholars were also central themes. Over the course of the panel, three key knowledge gaps were highlighted: the absence of effective theory linking cybersecurity to economic realities, the lack of relevant, reliable, or exploitable largescale data or data collection to effectively enable this kind of research, and the missing participation of economics scholars in cyber conflict debates.

Based on discussions there are no clear canonical works in this area; rather, there are works that could inform this type of research and the development of an authoritative body of academic literature. This review presents the three threads with associated questions raised in the discussion.

Creation of the Economic Impact of Cyber Threats Panel

This year was the first to feature a dedicated panel to discuss the challenges of cyber insecurity to economics. However, the panel was created in response to the scarcity of cohesive thought on the challenges of cyber insecurity and vulnerability to economies and societies. The objective of this panel was established to explore the potential challenges to existing economic theory and how to correct any theory shortcomings.

Takeaways from 2017

The inaugural Economic Impact of Cyber Threats discussed far-ranging topics and concepts, leveraging the diverse participants of the Cyber Conflict Studies Association. The breadth of topics discussed indicated a willingness to conceptualize of the panel's topic through a variety of methodological and theoretical lenses. However, this also meant discourse remained largely at higher, conceptual levels. Nonetheless, three major clusters of interest emerged through the panel discussion.

1. The first discussion area was oriented around the validity of the panel's core question regarding economic theory. These concerns fell into two broad categories. The first is that the problem is a fleeting or outside the scope of cyber conflict studies. Specifically, current challenges will either be resolved as cybersecurity becomes normalized or as status quo challengers. Countries like China will become more established and less inclined to tolerate or engage in malicious cyber activity. The second was that the topic was inherently within the realm of economics. Some argued that cyber threats to economies would be managed and treated like any other form of risk and managed accordingly and that this was not an issue of theory but time, that equilibrium would be restored. Others argued that these cyber challenges to specifically neoclassical economic models may be sufficiently critical and profound that they require a critical reassessment of existing foundational economic theory.
2. The second discussion area was how to effectively investigate the issues of cyber insecurity's effect on economies and what would be necessary to develop new economic theory, if necessary. These concerns followed one of three threads: definitions, data, and /or methodology. There was agreement that there needed to be a clearer, more precise use of terms when engaging in multidisciplinary research, as this would entail. Even during the discussion, there was debate over terms of reference, such as those associated with economic or accounting loss, among others. This highlighted the ongoing and well-known challenges of adopting a common terminology. Data was the largest issue, acknowledging that any research would require relevant and trusted data, which is extremely difficult to obtain given the covertness of cybersecurity operations generally and institutional reluctance to reveal information on breaches or other losses. Furthermore, establishing a collection regime, even with cooperative and trusted states and firms, is challenging. There is no consensus on what data is needed, the best methods for collecting it, and how to know if some critical data has been overlooked. There were questions on how to effectively and predictably quantify things like intellectual property theft. Finally, there were concerns raised about the methodology, establishing causality in areas as complex as national economies and cybersecurity, and most critically, what economic theory might be suspect and in what ways.
3. The final area of discussion was how cyber conflict studies could advance economic theory and role for future scholars, both in what types of

research could be done and how to make this line of research viable for academics, both established and emerging. A part of this was how to draw support and interest from economists to engage with the challenges of cyber conflict scholars.

2017 State of the Field: Economic Impact of Cyber Threats

Lack of Theorizing

While the economic impacts of cyber insecurity are becoming increasingly clear, there has been scant progress in developing theories to explain what the consequences this cyber insecurity is to national economies and systems. Cyberspace has facilitated global interconnectedness and revolutionized a host of fields, as well as giving rise to cyber conflict studies. However, there have been insufficient efforts to develop theories that span multiple disciplines in the same way that the impacts of cyberspace have changed the world they study. Economic theories, international relations theories, and theories of warfare need to be better integrated into the cybersecurity debates and vice versa. Emerging powers, such as China, and non-state actors utilize cyberspace in unintended ways that directly affect areas of interest to a range of academic disciplines. Despite the changing status quo, the guiding frameworks across these disciplines of studies continue to be generally fragmented in presumptions, logic, explanations, and policy conclusions.

Key Questions

- To what extent can—or should—cyber studies or cyber conflict studies be isolated from other fields?
- How do the economic definitions need to be adjusted or redefined for a cybered world and what then happens to related theories' applicability to the emerging world?
- What do the standard economic terms mean in the context of cyber conflict, such as—but not limited to—cost, value, rationality, harm, information, trust, tradeoffs, concepts of utility (marginal, optimal, etc.), and comparative/absolute advantage?
- What new theories or theoretical adjustments are implied if the fundamental (and highly westernized) rule of law—taken for granted in modern economic models—no longer applies or is not uniformly applied/enforced in a deeply cybered world dominated by nonwestern and more authoritarian states?
- What gaps in current models need to be filled, or new theories developed to deal with observed and rising volume of theoretically excluded or unaccommodated—and largely unrestricted—behaviors in cyberspace and cyber conflict? These behaviors include, but are not limited to: zero marginal cost industries thriving and able to charge non-zero prices, economic development advances through theft of intellectual property, the rise of cyber national champions, economic coercion of large and small enterprises by hostile cyber actors, the rationality of risk calculations by criminal non-state actors (both groups and individuals) in cyberspace, large corporations experiencing massive breaches and loss of IP capital , and states not exercising effective governance over the IT capital goods sector.
- How does cyberspace as an unprecedented substrate underlying both democratic and authoritarian societies challenge existing economic and conflict models? To what extent does it break, bend, or make irrelevant current theories? In what way and through what mechanisms do these challenges express themselves, from its scale globally, its speed in complex system interactions, its opaqueness in basic structures, to its enhancement of global system sensitivity to large coherent and aggressive actors seeking dominance over a few critical sectors like telecommunications?
- How can theories of future states be crafted from current economic models? How can those models help inform national leaders and policymakers who are struggling to keep pace with rapid technological advancements? How can theory help us prepare for destabilizing, disruptive, or destructive cyber-accelerated systemic surprises in the future?

Lack of Data

There are no norms, standards, professional sharing practices, or regulations that provide reliable and large enough scale macro- and micro- economic and cybersecurity datasets suitable for economic analysis. These challenges apply to other data scientists and even quantitative social science researchers as well. Mandatory reporting could help, but as yet, it is not clear what variables and data, and at what granularity, is needed to study the intersection of cyber conflict and economics properly. Questions that are not easily quantified—such as economic resilience to cyber threats or the effects of cyber on societal resilience will not necessarily be attractive to economists or viable for statistical analysis.

Key Questions

- What data forms, collection, variables, and reliability are required and achievable?
- How does one establish the wider systemic implications of cyber insecurity and economics without data? Are there credible and verifiable surrogates—reliably available over time—that may be used if the preferred data is unobtainable?
- What are the usual and unusual sources of useable and reliable data across nations, cultures, and use cases?
- How can measures such as losses in GDP terms be made meaningful—and therefore theoretically informing—with additional context and verified methods of collection and analysis?
- How can concrete cases of significant economic gains from economic distortions, such as the Huawei IP theft leading to the bankruptcy of Nortel—or the WannaCry/Petya ransomware—be more rigorously investigated?
- How can cyber incidents of varying magnitudes, types, and targets be integrated to understand the larger effects on economies? For example, given the Chinese role in cyber extractions and its meteoric national rise in global economic influence, to what extent is a new model of economic growth necessary, one suitable for a deeply cybered world?
- What data will help disentangle the benefits of cyber from other economic benefits and behaviors across regions, cultures, and demonstrated governance preferences?
- What data—and from where—is necessary to explore if new models, language, rules, and trend indices of international trade are necessary to capture changing global economies and markets accurately?
- What emerging computational or statistical methods might be modified to help address the data challenges, such as gathering non-traditional digital signatures information or massive dataset analysis?

Lack of Neoclassical and Political Economists in Cyber Conflict Studies

Cyberspace has taken root globally and become a common substrate to developed and developing economies and societies. However, neoclassical economists and quantitative political-economy scholars are absent in discussions of rising interstate conflict, massive illicit wealth transfers, changes in trade dynamics, and other systemic evolutions and surprises. Scholars, especially junior scholars, have begun to question the standing theoretical assumptions and conclusions in fields ranging from international relations, security studies, and psychology to systems engineering, and even the information technology disciplines. However, economists have shown less interest or initiative in questioning their theoretical foundations. The few who are challenging the current models—largely built in the Cold War era—are those with Nobel Economics awards like Robert Shiller or a small group of critical economics theorists researching what they call "real world economics."[1] Even those challenging the models are not, however, integrating cyber in their critiques or new theories. Despite massively disruptive cyber incidents, effects on companies and markets, and other cybersecurity costs imposed on citizens, societies, and increasingly antiquated laws intended to keep markets transparent and fair; research remains scant.

Why aren't economists interested in the economic impacts of cyber threats? One argument has been the lack of data discourages the ease of using the quantitative tools now required in academically credible economic analysis. Another possibility is each subfield of economics viewing cyber's impacts as another

field's problems. For example, massive intellectual property theft viewed as a firm-level problem only for micro-economists, or as a problem only for trade or macro-economists in that nations need better regulation and should use WTO mechanisms to arbitrate the costs and punishments. Leaving aside cyber, these three main fields in economics already are not integrated into approaches, and each is siloed conceptually, accepting for purposes of simplification the theoretical assumptions of the other two fields as given in the background of research. There is no incentive to include a systemic variable such as cyberspace which could be viewed as relevant to all three subfields.

Unfortunately, cyberspace does reach systemically across all varying levels of analysis in existing economics, micro, meso, macro, and trade. Economic models depend on simplification that may minimize distortions caused by systemic cyber vulnerabilities. The theories externalize systemic and background stabilization to governments and assume the norms of democratic civil society—from the assured value of currency to legal protection of contracts to policing of theft—are in full operation universally. The future also poses a problem in attracting economists to this field since they do not have tools to model the cyber in the future world. Cyberspace, as it has evolved, is creating even greater disparities between current models and theories and the emerging and conflictual surrounding reality.

Key Questions

- Why aren't existing economic assumptions being reassessed, as they are in many other social sciences?
- How can job opportunities exist for scholars looking at cyber economics at all, let alone the combination of cybersecurity, economics, and conflict?
- Does it hurt or help in attracting economic scholars to these questions if cyber economics is viewed as a distinct field, and how can the question of threats and conflict be included?
- What key terms—such as market failure and economic rationality—are particularly challenged in this space and how can the normal tools of neoclassical economists help them be sufficiently aware of these systemic changes?
- What is needed to have the political-economist become less focused on the political and more on the economic challenges and cyber in order to become the translating field of study in this area?
- What is the argument for and against having a separate subfield of cyberpolitical-economy in order to produce both integrating theories and large data collection necessary to fill the gaps in this space?

Summary and Recommendations

The key observation from this panel is that economics, while critical to the study of cybersecurity and cyber conflict, is woefully understudied by the scholars in economics. Making the case to that audience in particular about filling gaps in theories, data, and researchers is essential. There remains much to be done.

In the interim, recommendations for action include investigating potentially overlooked existing models whose data, methods, and theories could be adapted for use. Examples include information theories, socio-technical systems and surprise research, new forms of accounting (holistic), and works on normative synthesis. These and others could be drawn into use in this field to encourage openness to help acquire the missing data. The data problem will also require both an evaluation of the types of modeling done and what we consider viable data. As mentioned, there is a range of discipline that utilizes quantitative methods. Those fields also utilize diverse, and sometimes disparate, forms and types of data. Cyberspace is a digital space and is an abundant source of data, although not always in easily exploited forms or of obvious utility. However, using novel methods and models that abundance of data can be leveraged. Already we have seen the application of automation to collect, clean, and assemble massive datasets. Coupled with big data methods and analytics meaning can be derived to even apparently useless data. Assuming right question is being asked in the right way. This is just one example of an opportunity to derive important academic insights from novel methods and data sources.

Additionally, the literature on technological diffusion, corporate ventures, and cyber operations could be integrated to understand the role of cyber threats in changing inter-state relations. Making a case for how critical economics is to the conflict in cyberspace could be helped by investigating literature on economic coercion,

arsenal democracies, gains from invasions physically and (now) digitally, and engineering lessons on creating systemic reliability even when combining unreliable systems. To help incorporate the work of other academic disciplines into cyber conflict studies will require both a willingness to accept existing lexicons, but also the willingness to adopt baseline terms and theoretical constructs. It is challenging to involve academics with diverse research backgrounds, such as economists, into the cyber field when their lexicon is inaccurately used and when the cyber lexicon is always in flux.

The bottom line is that cybersecurity scholars need to reach out and persuade economists to vigorously engage in the rising challenges of a deeply conflictual cybered world. That persuasion will take a while, and there are many urgent questions to be answered across this space. There are other fields that also need to be considered, and some may offer complementary data and explanations that lead to unexpected and supportive discoveries for all the disciplines involved.

About the Authors

Chris C. Demchak, Ph.D., is the RDML Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College.

Benjamin Schechter is a research associate at the Center for Cyber Conflict Studies(C3S), U.S. Naval War College.

End Note

1. See for example the Real World Economics Review website, www.worldeconomicsassociation.org/journals/rwer/

Relevant Literature

While limited academic attention has been given to the issues raised in this panel, there is a relevant body of literature that can help inform future research into these issues. The literature presented here is not exhaustive but represents the first steps into exploring the systemic effects of cyber insecurity on economic theory.

Relevant contributions to Theorizing Gap

Holling, C. S. (2001). "Understanding the Complexity of Economic, Ecological, and Social Systems." *Ecosystems* 4(5): 390-405.

Parsons, T. and N. Smelser (1998). *Economy and society: A study in the integration of economic and social theory*, Routledge.

Baldwin, D. A. (1985). *Economic statecraft*, Princeton University Press.

Kahn, A. E. (1966). "The tyranny of small decisions: Market failures, imperfections, and the limits of economics." *Kyklos* 19(1): 23-47.

West, G. (2017). *Scale: The Universal Laws of Growth, Innovation, Sustainability, and the Pace of Life in Organisms, Cities, Economies, and Companies*. London, Orion Press.

Wang, Z. (2017). "The Economic Rise of China: Rule-Taker, Rule-Maker, or Rule-Breaker?" *Asian Survey* 57(4): 595-617.

Bloom, N., et al. (2013). "A Trapped-Factors Model of Innovation." *The American Economic Review* 103(3): 208-213.

Roe, E. (2012). *Taking complexity seriously: policy analysis, triangulation and sustainable development*, Springer Science & Business Media.

Relevant contributions to Data Identification and Acquisition Gap

Li, Z., et al. "Botnet economics: uncertainty matters." *Managing Information Risk and the Economics of Security*: 245-267.

Hannas, W. C., et al. (2013). *Chinese industrial espionage: Technology acquisition and military modernisation*, Routledge.

Relevant contributions to Missing Incentives for Economists Gap

Kakerlof, G. A. and R. J. Shiller (2015). *Phishing for phools: The economics of manipulation and deception*, Princeton University Press.

Keen, S. (2011). *Debunking Economics: the naked emperor dethroned?*, Zed Books Ltd.

Mishan, E. J. (2011 (1986)). *Economic Myths and the Mythology of Economics* (Routledge Revivals), Routledge.

Blanchard, O., et al. (2012). *In the wake of the crisis: Leading economists reassess economic policy*, MIT Press.
Akerlof, G. A., et al. (2014). *What Have We Learned?: Macroeconomic Policy After the Crisis*, MIT Press.

Romer, P. M. (2015). "Mathiness in the Theory of Economic Growth." *The American Economic Review* 105(5): 89.

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.