Crossing the Digital Divide: Monism, Dualism and the Reason Collective Action is Critical for Cyber Theory Production

Whyte, Christopher

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Whyte, C. (2018). Crossing the Digital Divide: Monism, Dualism and the Reason Collective Action is Critical for Cyber Theory Production. *Politics and Governance*, *6*(2), 73-82. https://doi.org/10.17645/pag.v6i2.1338

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 73–82
DOI: 10.17645/pag.v6i2.1338

Article

Crossing the Digital Divide: Monism, Dualism and the Reason Collective Action is Critical for Cyber Theory Production

Christopher Whyte

L. Douglas Wilder School of Government and Public Affairs, Virginia Commonwealth University, Richmond, VA 23284, USA; E-Mail: cewhyte@vcu.edu

Submitted: 31 December 2017 | Accepted: 12 February 2018 | Published: 11 June 2018

Abstract
In studying topics in cyber conflict and cyber-security governance, scholars must ask—arguably more so than has been the case with any other emergent research agenda—where the epistemological and ontological value of different methods lies. This article describes the unique, dual methodological challenges inherent in the multifaceted program on global cyber-security and asks how problematic they are for scholarly efforts to construct knowledge about digital dynamics in world affairs. I argue that any answer to this question will vary depending on how one perceives the social science enterprise. While traditional dualistic perspectives on social science imply unique challenges for researcher, a monistic perspective of Weberian objectivity does not. Regardless of one's perspective, however, the most important steps to be taken at the level of the research program are clearly those focused on constructing the trappings of community. To this end, I outline steps that might be taken to develop a range of community-building and -supporting mechanisms that can simultaneously support a micro-foundational approach to research and expose community elements to one another. Doing this stands to better opportunities for the production of knowledge and direct researchers towards fruitful avenues whilst shortening gaps between the ivory tower and the real world.

Keywords
cyber; dualism; epistemology; monism; ontology; philosophy of science

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

For almost half a century, new information and communications technologies (ICT) based on packet-switching and related network-oriented design features have worked to rewire the international system. The digitization of global infrastructure has transformed the constitution of global commerce, social connections and security relationships alike. Given the scope of the impact of this most recent information revolution, it seems reasonable to assert that cyber-security—i.e. the security of socio-technical systems and, more specifically, practices involved therein—is, thus, a policy field aimed at more than *only* technical, organizational or national security. Wherever ICT undergird societal functions, questions of cyber-security abound. And, since ICT have also augured unique changes to the global information environment, cyber-security analyses and prescriptions must necessarily consider the broader intersection of technology and the normative fabric of world affairs. In short, the scope of the scholarly research program on cyber-security governance, conflict and economics is immense.

And yet, the broad field of cyber issues studies faces unprecedented foundational challenges with respect to the construction of new knowledge. Specifically, and perhaps moreso than has been the case with any other emergent research agendas in recent history, scholars studying cyber matters must consistently grapple with distinct epistemological and ontological questions. Given the inherent difficulties in obtaining data and validating observational inferences, how can we presume to know what we think we know? If the link between our empir-

ical resources and inferred findings is open to question, how can we be sure that the phenomena and dynamic forces we study are as we see them? All social scientists must confront such issues in their approach to understanding the world around them and, from Hutchins (1995) seminal work on cognition to Mindell's (2002) cybernetics exploration of interacting control systems, there exists a rich literature on both the challenges and value proposition inherent in studying the interaction of technology and human systems.

But with cyber-security issues the potential obstacles are uniquely pronounced. While it is certainly possible to study, for instance, traditional questions of bureaucracy and politicking around Internet-oriented bodies without considering technological variables, a great deal of work is inevitably aimed at assessing technology as it supports, impacts and enables kinetic human interactions. As such, a substantial element of the academy in this area must attempt to link technological empirical foundations with socio-physical outcomes.

This article asks how problematic core methodological challenges commonly identified by cyber-security researchers really are and describes steps that might be made to improve prospects for knowledge construction at the level of the research program. Over and above environmental problems in obtaining data, the cyber-security research program suffers from acute attributional challenges. To date, scholars employing data obtained through public-sphere observation or in collaboration with technology vendors have taken one of two approaches to data collection, with scope conditions being set by either socio-kinetic or technical system details. Though both approaches are promising, the basis of each suggests inherent challenges in cross-validating results and building macro theory. It is often extremely hard to attribute digital patterns to sociopolitical wherewithal; likewise, inquiry that selects on specific actors in world politics is often unable to capture the scope of covert digital actions. In essence, though existing research certainly stands to contribute to the body of knowledge on cyber politics and cyber-security governance, contradictory bases for investigation combine with the domain's unique attribution challenges to make analysis of sociopolitical phenomena systematically difficult.

The challenges before the multi-faceted cyber research program are not new and are novel only insofar as ICT regularly produce a disconnect between domain-specific actions or outcomes and real world ones. In truth, the question of methodological approach to cyber issues is one of reconciling existing perspectives with advancing work in such a way as to develop a scientifically healthy research program. In the sections below, I describe competing perspectives on the ability of social science approaches to build a body of knowledge that impartially describes the real world. I point out that while dominant dualistic perspectives on social science suggest that attribution challenges for empirical work in the cyber field are severe, a monistic interpretation of the social science enterprise implies they are problematic only insofar as scholars should ideally be able to gauge the shape of all elements of the real world for purposes of forming impressions. I then argue that, regardless of the perspective one adopts, scholars in the burgeoning cyber-security research program should take steps to develop a range of community-building and -supporting mechanisms that can simultaneously support a coordinated micro-foundational approach to knowledge construction and expose community elements to one another. The sections below outline the case for this in greater detail and make a series of specific recommendations.

The remainder of this article proceeds in five parts. First, it considers the nature and aims of the cyber-security research program within the social sciences. Then, it briefly discusses competing philosophical perspectives on the constitution of knowledge in research on the world around us and fleshes out unique, dual attributional problems that many researchers must inevitably face in efforts to link technical foundations to socio-physical context. Thirdly, the article discusses open source research in the broader program of investigation and adjudicates on the degree to which unique attributional problems matter. Finally, it argues that, regardless of one's perspective on the nature of the social science enterprise, a community-oriented organization of research efforts is critical for efforts to construct macro theory and generate meaningful inference. Here, I make specific suggestions at the level of the research program, before concluding.

2. The Shape and Focus of Digital Studies Research

Cyber studies constitute an immensely broad field of investigation. This is a necessary condition because of the unique foundational feature of the network technologies that lie at the heart of the field. Simply put, changes to global society in this most recent information revolution have emerged from a multiform application of new design features to the full range of societal infrastructure. Information technology is crosscutting to such a degree that it is the rare social, political or economic issue that has not been impacted. As such, cyber studies possess an incredible broad substantive remit. At the highest level, we might consider this remit to include the dynamics of technology adoption across global society (Choucri, 2012), the role of governments in problematizing and meeting cyber challenges (see among others, Knake, 2010; Nye, 2014; Stevens, 2017), the resultant management of international security and the fundamental institutional, technological and societal prerequisites of security.

Though it might otherwise do to categorize the cyber studies research program into different academic areas of focus, from global cyber-security governance (Choucri, Madnick, & Ferwerda, 2014) and cyber conflict mechanisms (see among others, Buchanan, 2017; Gartzke & Lindsay, 2015; Valeriano & Maness, 2015) to the organization of social movements in virtual spaces (for in-

stance, Beyer, 2014) and the cutting edge of ICT development, the fact of the matter is that methodological issues and imperatives in this vein emerge from a simple proposition—that the most recent information revolution has fundamentally altered not only the nature of human interactions on a global scale, but also the constitution (i.e. the context) thereof. If this proposition is accurate or even accepted in part, then the field's remit is truly unique. Different from research sub-programs across the social sciences that study specific tools of human interaction, the study of world politics as couched in the context of ICT adoption and integration is the investigation of transformed environmental conditions on a global scale. Though man-made, the evolving digitization of global infrastructure presents as *both* an exogenous determinant of human interconnections and an endogenous modifier of specific relationships.

It would not do here to go on without recognizing that there exists a rich and well-trodden literature on the interaction of human institutions and the tools they employ. Nestled in the field of science and technology studies, research on cybernetics has for many decades described the manner in which technology is not simply a material feature of the world that humans engage with in the course of our actions (see among others, Mindell, 2002; Mindell, Segal, & Gerovitch, 2003; Wiener, 1961, 1988). Rather, technology is a tangible variable that both shapes human agency and determines the normative context of human interactions (Hutchins, 1995). What's unique about the most recent information revolution is the twofold manner in which new ICT both provide for human interaction substantially detached from real world context and do so systematically at the global level. Thus, while literature that takes reference from work on cybernetics, social network theories and more is relevant to the research program on cyber-security—and, indeed, has recently been the focus of a handful of unique contributions to the field—the methodological challenges facing scholars today is of unique scale.

The result of such a dynamic is reasonably clear. Though, again, it is possible to study cyber effects without looking beyond what some have called the "real-kinetic" empirical dynamics of world affairs (Choucri, 2012), much of the broad-scoped cyber studies research program will enduringly be required to look at the intersection of specific ICT usage, implementation dynamics and resultant human behavior. In reference to a well-developed program of study on the nature of power and position in international relations (Barnett & Duvall, 2005), it seems reasonable to bound such work in two ways. First, much cyber-security research aims to understand how ICT play a role in augmenting human interactions of various kinds. Some, for instance, has attempted to map out the shift in how humans and human institutions problem-solve given today's global network-centric environment (see among others, Amoore, 2009; Dreyfus, 2008; Galloway & Thacker, 2007; Shaviro, 2003). Here, researchers are already grappling with the challenge of matching data on the use of ICT with a range of sociopolitical outcomes. And again, as is broached further below, there exists in cybernetics scholarship a nuanced basis for examining closed systems of technology incorporated into human structures. Second, yet other work aims to understand how ICT might act to alter—either directly or reflexively through societal reactions to the information revolution—the context of those interactions. Here, a range of research sub-programs in the psychology, biology, business and sociology fields has emerged to assess the manner in which the most recent information revolution has fundamentally changed patterns of human behavior. In both cases, the need to link information on direct human interactions with ICT to related outcomes is clear. Across the board, however, this imperative presents as a unique challenge wherein attribution of digital actions to various kinds of outcomes is not only difficult methodologically, but fundamentally linked with scholars' ability to infer.

3. The Digital Divide: With Cyber Research, How Do We Know What We Know?

When it comes to linking human behavior enabled via use of ICT, there are two distinct challenges for the researcher. One of these is technical, the other preferential. The first is that links between digital realities and human actions are tenuous. Whether the subject of focus is patterns of cryptocurrency usage (Sat, Krylov, Evgenyevich, Kasatkin, & Kornev, 2016) or the attribution of cyber attacks (Rid & Buchanan, 2015), tying evidence of digital behavior to human input is difficult. The second challenge is that resources necessary for doing so are often hidden behind not only technical barriers, but also socio-institutional ones.

With regards to attribution of cyber activities, much has been written across both the technical and social sciences. For the purposes of social scientists, it is enough to say that attribution of digital actions can be immensely challenging simply because of the layered manner in which relative ease in masking digital signatures meshes with the additional difficulties involved in linking virtual actions to human behavior (Guitton & Korzak, 2013). Technical attribution—i.e. the linking of cyber actions with indicators of action instigated by humans or human-programmed systems—is not dichotomous. It would be disingenuous to say that a measure of technical attribution of digital actions either does or does not point the finger at specific causes of disruption or compromise. Attribution short of linking ICT usage to human agency runs the full gamut from technical abilities to convince investigators of a given pattern of action to the much rarer ability to lay out a case that an informed public audience would be hard pressed to argue with (Geers, 2010). This is made yet more problematic given that opponents are not unitary. As Rid and Buchanan (2015) point out in their discussion of Moonlight Maze as an example, efforts to confirm attribution evidence pointing to Russian security

services ran into the problem of a clear compartmentalization of knowledge of offensive operations within the Russian government. Some operators knew about the expansive espionage campaign; many did not.

And yet, when it comes to attribution of digital actions, technical demonstration of the origination thereof is just part of the challenge. Indeed, it is arguably the lesser part of the challenge. Even where data is made available wherein technical attribution is possible to a high degree of certainty, there inevitably exist additional certitude problems for any scholar or analyst attempting to link digital actions to sociopolitical ones. For scholars, such intelligence gathering as a component part of cyber research is particularly challenging, as we must often trust (given a certain ability to control for uncertainty) the nature of information that attributes particular actions to actors. This naturally speaks to a higher-level problem with the attribution of digital dynamics to real-kinetic ones such that research on the broad gamut of digital issues are faced with unique ontological problems, namely that sources and providers of relevant information suffer from a broad range of measurement and reliability problems.

In research on cyber conflict, in particular, it is apparent to a broad range of scholars that barriers across which lie the ability to generalize about digital actions are more opaque than they are with traditional areas of security work (see among others, Kello, 2013; Rid & Buchanan, 2015; Valeriano & Maness, 2014). The nature of global network infrastructure as being substantially privately owned means that access to Internet traffic data and innumerable related metrics is hidden behind preferential access walls. In essence, robust analysis is difficult for those operating in the public sphere because we must contend with the incentives that both private industry and government operators have to either not report or misrepresent what they know about the digital domain. Private firms must consider their reputation, their standing with stakeholders, the value of their intellectual property and a maze of compliance requirements when deciding how to report information and whether or not to share data with academics and the public (Byres & Lowe, 2004; Sgouras, Birda, & Labridis, 2014). Moreover, operators willing to share relevant data for use in research often enforce rules about how data can be used (to enhance their public standing, for instance) and government sub-organizations inevitably favor intelligence and defense community research in their decision-making. What topics of interest do not suffer from this issue—such as the use of ICT by activists for inherently public-facing efforts (see, for instance, Morozov, 2012; Shirky, 2008; Yang, 2009)—are virtually unique in that observation of digital actions does not require interaction with a gatekeeper of some kind.

These dual challenges to research progress constitute a digital divide wherein linking observation of digital dynamics to sociopolitical corollaries is systematically difficult, both technically and logistically. Given these foundational challenges with linking the growing base of knowledge about a range of digital issues with actual patterns of human interaction in the digital domain, how can scholars possibly know what we think we know (Jackson & Nexon, 2013)? In particular, beyond the scope of individual projects that find unique ways to obtain, validate and employ data, how can an entire field of study act to remedy the clear problem of socio-technical gatekeeping that mires research—in the aggregate—in ontological uncertainty?

4. How Problematic Are Such Challenges? The Dualist and Monist Perspectives

To consider these questions, it is necessary to consider different philosophical perspectives on the nature of social science and the development of effective research programs. Broadly, effective assessment of a research program's health and viability demands consideration of the nature of the relationship between knowledge held and assumed by scholars, on the one hand, and the empirical nature of the world around humans on the other. Do our observations and subsequent inferences accurately describe the real world? Or do they, since human consciousness and operation is inherently a function of the subjective way in which our minds view particular parts of the world, lead to the development of a base of knowledge that only makes sense in the context of human biases and interpretations? Recognizing these competing perspectives and subsequent implications for the knowledge generation process is critical for adjudicating on the best paths that might help remedy the cyber-security research program's inherent ontological challenges.

To be clear, in the immense literature on the philosophy of science (and particularly on the ontological challenges of scholarly research), the questions posed above in no way suggest some division between an idealistic view of knowledge creation by researchers and a more pragmatic one. The assertion that human stores of knowledge do not accurately reflect the world around us is simply a function of recognizing the role that prior knowledge plays, in the form of biases and preconditioned modes of problem solving, in shaping research design and interpretation (see among others, Bennett, 2013; Lake, 2011; Sil & Katzenstein, 2010). In assessing a unique dynamic scientifically, researchers are invariably prompted to address methods, practices and results that the broader research community assess are adjacent to the current venture. And regardless of how effective a given research design is at preventing the introduction of bias, interpretation of results and the subsequent task of placing new knowledge in the context of a broader knowledge base inevitably prompts researchers to interact with a broader construct (Habermas, 1987). This is particularly the case given that interpretation of results is rarely the task of individual researchers or investigative teams, but is inevitably at some point a task undertaken by broader elements of a research community

that need not observe scientific controls in their attempt to consensually place new knowledge amongst the rest. The result is a disconnected body of knowledge that only represents the real world in the context of the practices of those who developed that knowledge in the first place (Jackson, 2008). This notion of the relationship between empirics and human knowledge is called *dualism*.

By contrast, *monism* pushes back on the narrative of dualism as reflecting an inevitable divergence in the shape of the real world and human understanding of the real world. Monism is the perspective that human knowledge and the real-kinetic landscape of the world around us are one and the same (Weber, 2017). This is not because advocates of monism reject the notion that bias can infect and skew the results of the scientific enterprise. Rather, monists recognize that the parameters of what humans *might* understand about the world around us is inherently a function of how we categorize "things" in the world (Weber, 1904). Humans give meaning to what we are studying by identifying them to begin with. Thus, focusing purely on real-kinetic events, dynamics and fundamentals in the world around us allows us to understand *both* the "things" that we understand to be in the world (i.e. the landscape of the world around us) and the knowledge we hold about those things (Jackson, 2008). Whereas dualism holds that there is an objective reality about the real world that is separate from human knowledge of the world, monism holds that understanding critical junctures and events via observation allows us to understand the world in such a way that our body of knowledge is essentially congruent with the condition of the world.

The debate over the nature of the social science enterprise between monists and dualists has seen a range of developments in recent years. Pushing back against the correlative narrative of both classical and seminal dualists, in particular, a series of works (for instance, Bennett, 2010) and conference publications (Mackay, 2007) have organized around the concept of factual or speculative materialism. Advocates of such thinking propose that objects are not elements of "the real world" to be assessed and characterized as one thing or another, but are multi-factual constructs as potentially complex as human beings (Bryant, Snricek, & Harman, 2011; Phetteplace, 2010). Thus, far from accepting the notion that inferential analysis cedes knowledge about a world in which humans operate, speculative materialists (or realists) join others in conceptualizing systems wherein humans are not unique as animate objects.

5. Dualism and Monism as Competing (Approaches to the) Social Sciences

In a discussion of the ontological challenges faced by the cyber-security research program, why should we care about competing philosophical perspectives on the nature of the social science enterprise? Simply put, advocacy of one or the other leads to a diverse set of prescriptions on what kinds of scholarly activities are most likely to build a useful, accurate and accessible store of knowledge by the academy. The shape of such activities, in turn, suggests the degree to which the challenges inherent in undertaking empirical work on many cybersecurity topics are problematic for the development of the research program.

Dualist perspectives on the social sciences are, by far, more commonplace than are monist ones. Though most social science work from the mid-20th century onwards tends to self-describe as "positivist" (or variations thereof) in nature, the reality is that most scholars reject the notion that observation is synonymous with the shape of the real world. Rather, most are dualists of one kind of another that essentially seek to dispense with the character of their own perspectives in order to better understand empirically the environment in which humans exist and interact. Again, though most social scientists today would likely identify as positivists, the better term to use would, according to Jackson (2008), be *neopositivists*.[1] Such scholars, divided as they are on a range of philosophical points (see Blaug, 1975; Fuller, 2004; see also Kuhn, 1970; Popper, 1970), nevertheless uniformly reject the monism of positivism and agree to the central importance of one particular scholarly activity as critical for the generation of knowledge that increasingly describes the real world accurately—falsification (Lakatos, 1976). Falsification, simply put, is the design of observational scientific procedures such that different hypothetical suppositions can be rigorously tested and eliminated if certain conditions are not met. It is an activity that, by definition, dictates the existence of a divide between human activity in research practices and the world around us.

By contrast with prevailing dualist perspectives on the social sciences, monist ones reject the entire notion that what we see in the world around us is some kind of neutral tapestry on which humans draw and from which we take reference. As Jackson (2008) describes, monism's most well-known proponent—Max Weber—argues that there can be no social science enterprise without pre-defined and assumed socio-cultural understanding of what is actually under study (Weber, 1904). Here, Weber addresses the most common criticism of dualist—and particularly neopositivist—approaches to research. Since neopositivism necessitates the dispensation of human inputs to the observational process through some form of falsification in research design, it intrinsically demands some kind of agreed-upon standards of evidence and objectivity. In a comparative study, this would manifest in one or several agreed-upon methods for operationalizing both the dependent and inde-

[1] Though they are awarded singular focus in treatments of dualistic perspectives on the social science enterprise, neo-positivists are not alone in their view of human knowledge and real world dynamics being inherently separate. Jackson (2008) describes both critical realists and "partisans of 'communicative action'" (p. 130) as belonging in the dualist category.

pendent variables. This, of course, is the greatest weakness of dualism as social science. There is simply no way that scholars can confirm the validity of a given hypothesis, no matter the amount of otherwise seemingly-robust testing it endures, as *more correct* in its representation of the world around us (Hacking, 1999). Moreover, the requirement that researchers pick some measurements of the real world over others inherently weakens the falsification process in some instances in that hypotheses may constitute conventional wisdom or consensus positions in its parts. Such hypotheses might survive in scholarship because its construction is uncontroversial, regardless of the shape of evidence brought to bear. The Democratic Peace Theory is a paradigmatic example of such a hypothesis wherein the component elements are (or at least were for many years) broadly considered common sense without further operationalization (see among others, Layne, 1994; Risse-Kappen, 1995; Rosato, 2003).

The solution to such an inescapable inability to ever perfectly, objectively describe the world around us, according to a monist perspective on the social science enterprise, would be not to try. Rather than focus on accurately describing the world around us as a set of facts, scholars should assess ideal-type constructions of our world with consistent analytic premises (Lindbekk, 1992). These premises need not be free of bias in any way, but simply must be consistent and logically applied across research (Jackson, 2008). Such work is then judged to be more or less meaningful to the broader body of human knowledge given the degree to which is can successfully persuade an audience of diverse persuasions. In other words, good social science is that which can persuade the most people that hold contradictory perspectives on how the world works. Already in the well-dispersed literature on the information revolution, there are examples of monistic research designs implemented in compelling and robust fashion (see among others, Anderson, Kearnes, McFarlane, & Swanton, 2012; Balzacq & Dunn Cavelty, 2016; Berry, 2015). Whereas empirical efforts like those of Valeriano and Manesss (2015) rely on a series of assumptions external to the methods and data employed in analysis, work that draws upon socio-spatial theories and frameworks is able to nest assessment of a given phenomenon within fixed parameters only relevant to the study at hand. As a result, while opportunities for correlative findings pertaining to such phenomena are lacking, there are clear pathways to thick description thereof.

6. Open Source Research and Challenges for the Development of the Research Program

Given these competing approaches to knowledge generation and the organization of research programs, how problematic are barriers to effective observation of digital dynamics for researchers? While it is possible that individual researchers, research teams and institutions might find access to proprietary information that allows for unique analysis of a given phenomenon, the reality is that most investigation in the cyber-security research program is done—and will enduringly be done—off the back of open source data collection. Whether mining event data from news reports and wire feeds (as in Radford, 2016) or conducting ethnographic research into the shape of communities and institutions (as in Sowell, 2012), social scientists interested in undertaking work in this domain must largely do so absent the special access conditions held by stakeholders in the domain. Academic researchers may occasionally be allowed unique access to private data (for instance, King, Pan, & Roberts, 2013; Kostyuk & Zhukov, 2017) and are often supported by grants that enhance the power of observation at the level of the researcher, but they do not hold specialized roles—as do Internet service providers, intelligence entities or private cyber-security vendors, for instance—that might enduringly allow for access to information that could serve to bridge the attribution gap described above. A range of promising work has been done in the social sciences that empirically selects on either sociopolitical dynamics (for instance, Valeriano & Maness, 2015) or technical details (e.g. Mezzour, Carley, & Carley, 2015) as the basis for generalizing about a given phenomenon. In almost all cases, however, there exist clear shortcomings in the ability of researchers to validate their findings such that inference is possible. And while some creative solutions exist that have bridged the digital methodological divide at the level of discrete research projects, it is difficult to see how such challenges might be remedied at the level of the research program.

For dualists, the specter of such an enduring organizational and validating challenge in cyber research is particularly problematic. How research programs should and do emerge is hotly debated by both seminal and contemporary dualist philosophers, but the general idea is that research programs are layered constructions of knowledge wherein peripheral hypotheses linked with core theses are tested in order to advance the state of a given field (Jackson, 2008). Sometimes, hypothesis testing leads to such rapid advancement in the shape of specific knowledge that there is a revolution in general knowledge—in the theoretical bases of a research field. The manner in which this occurs is the subject of classical debate between thinkers like Kuhn and Popper. Regardless, the idea is roughly similar across the board and so it is easy to see why ontological problems in work focused on ICT and their impact dominate so completely. Systematic barriers to the robust implementation of falsification-based research designs are an impediment to the process of knowledge construction. Adding to this, the cyber-security research program is still in its infancy. The shape of general knowledge at the heart of the research program is unclear, suggesting that efforts to improve our knowledge base by rejecting pre-existing theory are premature and that, moreso than is common with established areas of scholarship, there is a strong imperative to articulate macro-theoretical perspectives. Taken to-

gether, the path ahead for efforts to construct an effective dualist social science research program is laden with likely pitfalls and uncertainty.

For monists, these challenges are less severe. Again, the monistic position is that scholars should assess ideal-type constructions of our world with consistent analytic premises rather than simply aim to describe the real world as a set of facts. As long as a researcher's premises are consistent and logically applied across research in the form of a clearly delineated analytic framework, good social science work is possible. The point is simply to persuade the most people that hold contradictory perspectives on how the world works. From this point of view, objective research on and around the cyber domain is entirely possible without specific systematic remedy to the ontological problems inherent in observational work across the board. Indeed, some such research is already emerging. Though it does not generalize on global patterns of cyber conflict, Balzacq and Dunn Cavelty's (2016) exploration of the applicability of Actor-Network Theory (ANT) demonstrates the manner in which network functionality and control can be shaped by fluid syntactic threats in the form of malware.[2] Such work has clear value to strategic planners. Punctuated successes like this that bridge the digital divide are as meaningful for the research program as would be a broad-scoped revolution in approaches to cross-validation and data obtainment within the field. Certainly, a monistic perspective might recognize that any effort to advance access to the means of observing all aspects of the domain is conducive to good social science insofar as greater exposure to information about the world will lead to a proliferation of world views and, thus, incentivize the production of more compelling analytic work. But lack of full observational data about the world around us is not necessarily a hard barrier to continued development of the research program. Indeed, even given a revolution in methods of approach to correlative research, speculative investigation seems better suited to providing scholars the means to consider the validity of non-obvious relationships.

7. Recommendations: A Need for Community and Collective Action

Obviously, the field of scholars interested in conducting cyber-security research—broadly construed—is diverse and destined to be constituted of elements that value different approaches to knowledge construction. This is perhaps more the case here than with other traditional fields of study within the social science enterprise given the degree to which the most recent information revolution has transformed the social, political and economic substrates of world affairs in a crosscutting fashion, attracting students of varied interests and research inclinations. Nevertheless, I argue that there exists a set of steps to be taken that addresses the imperatives of competing philosophical perspectives on approaches to be taken in such research in common. Specifically, these steps involve the construction of strong community mechanisms around the research program that can *both* encourage adoption of a micro-foundational framework for developing new dualistic research projects and expose diverse scholarly sub-communities (and their perspectives) to others in such a way that expands prospects for what monists might call a robust social science focused on cyber-security issues. Indeed, I posit that developments akin to those suggested below are necessary for the viability of a cross-cutting digital studies research program specifically because knowledge construction at the level of the program is impossible—regardless of a given scholar's dualistic or monistic conceptualization of the social science enterprise in this vein—without consensus and the mechanisms thereof.

Scholarly Responsibility. To some degree, the simplest mechanism for advancing the research program is quite simply continued and improved commitment to responsible scholarly practices at the level of the researchers and the research project. At present, the diverse cyber-security field is a somewhat fragmented beast insofar as best practices are not determined via reference to the research program so much as they are via reference to the traditional academic domains from which individual researchers hail. This is no clearer than with the case of standards for replication of investigatory work and hypothesis testing. At least at the level of the researcher, a voluntary commitment to adopt in-group replication as a basic standard for publication of evidence would help remedy the clear issue that arises from unique proprietary access to data that cannot be publicly provided. In essence, a commitment to allow an independent group of collaborators *not* co-investigating a given project should be common practice as a means for controlling for lack of replication options during and after the publication process (where data from vendors, interviews, etc. are used in a central role). Pre-publication replication would make work more credible and would tie scholarly reputation to a given research finding beyond what author(s) or results-*sans*-data might. Secondarily, the field should adopt standards for claiming inference from the medical and psychology fields wherein multiple independent studies (i.e. datasets) are employed and rated based on their credibility (see Francis, 2012; Maxwell, Lau, & Howard, 2015). Naturally, such efforts should be supported and bolstered via the purposive organization of research forums and conference programs around such principles of community cross-validation and debate. Likewise, jour-

[2] For a full introduction to ANT, see Latour (2005). Latour outlines ANT as both related to and a pushback against the monism described by Jackson (2008) and others. Latour sees most social science as being overly laden with suppositions about the character of actors and objects in world affairs. In essence, he argues for austere form of approach to understanding sociological assemblages—including security assemblages—in the world based on a materialist view of connections that cede meaning.

nal special editions and special conference proceedings would do well to be planned across outlets in coordination with such forums.

Common Resources. Further, the cyber-security research program should support efforts to build common resources for coordination. Particularly given that the field largely lacks core theoretical division in the way that traditional academic areas of focus do at this juncture, a micro-foundational approach to the production of knowledge—regardless of one's perspective on the nature of good social science—is necessary for the construction of robust foundations for future research. In this vein, coordination across diverse university researchers, centers and counterparts in the private sector is critical if the field is to both avoid rampant duplication of efforts and effectively encourage commitment to new research pathways in a timely fashion. To this end, the community should embrace the incorporation of both new technologies and mechanisms of cooperation found in the natural sciences. To the latter point, inter-scholar discussion groups like those found in the security studies and comparative politics fields should be encouraged via the patronage of organizing associations and full support should be lent to an effort to build a common repository for storing published work and relevant data. To the former point, the field would do well to consider the use of a collaborative blockchain-based system for sharing computing resources and cataloguing research interactions in a public, transparent manner.

A Digital Studies Scholarship Cooperative. Of course, without some kind of organizing force, much of this lies in the realm of suggestion free from an ability to effectively implement at the level of the immense community of scholars and institutions that constitute the cyber-security research program. I argue that such an organizing force, however, should not simply take the form of an association that primarily organizes conferences and provides professional resources to scholars. Rather, because of the unique methodological and coordinative challenges facing the field, I argue that scholars would be best served by participating in a digital studies research cooperative wherein the sole purpose is to enhance the clout and research prospects of the community-at-large. Secondary to a professional association, such a cooperative would be centralized only around an oversight committee of rotating membership that (given relevant review) acted to vouch for scholars negotiating for proprietary data access, ensured protection of such data, allowed for robust implementation of replication standards without violation of non-disclosure agreements and maintained the means for research/resource collaboration suggested above. Regardless of researcher priorities, developing such a cooperative would bring a broad set of benefits for researchers to all, not least the maintenance of a platform for coordinating the storage of new knowledge and orchestrating necessary collaborations amongst scholars undertaking related—even if methodologically distant—investigations.

8. Conclusion

This article has broadly sought to describe why unique attributional and availability challenges in the diverse research program on cyber-security are problematic. In particular, I have sought herein to highlight the monist perspective—an objectivity-based interpretation of the nature of knowledge construction championed by Max Weber—on what constitutes good social science. For monists, the challenges inherent in trying to bridge the digital divide in research are not, fundamentally, impediments to the development of a research program as is often seen to be the case among those of a more dualistic perspective on the social science enterprise. While enhanced abilities to cross-validate technical and sociopolitical observations—as well as to obtain data from otherwise opaque stakeholders that often possess such information—is desirable in general, it does not mean that the research program is doomed to enduringly be on shaky ontological ground. Rather, what is most desirable for the research problem is an expansion of community-supporting features of organization that will allow for better exposure of different world views expressed in analytic frameworks employed in research. Fortunately, such an approach is highly compatible with the imperatives of the research program as dualists might articulate them. Focus on better cooperative organization within the field stands to improve broad commitment to research standards and encourage the development of much-needed provision of common resources for the scholarly community.

Acknowledgments

The author would like to thank both reviewers and the Academic Editor for their comments and suggestions on the work presented in this article.

Conflict of Interests

The author declares no conflict of interests.

References

Amoore, L. (2009). Algorithmic war: Everyday geographies of the war on terror. *Antipode*, *41*(1), 49–69.

Anderson, B., Kearnes, M., McFarlane, C., & Swanton, D. (2012). On assemblages and geography. *Dialogues in Human Geography*, *2*(2), 171–189.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–98.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International organization*, *59*(1), 39–75.

Bennett, A. (2013). The mother of all isms: Causal mechanisms and structured pluralism in International Relations theory. *European Journal of International Relations*, *19*(3), 459–481.

Bennett, J. (2010). *Vibrant matter a political ecology of things*. Durham, NC: Duke University Press.

Berry, D. M. (2015). *Critical theory and the digital*. New York, NY: Bloomsbury Publishing.

Beyer, J. L. (2014). *Expect us: Online communities and political mobilization*. Oxford: Oxford University Press.

Blaug, M. (1975). Kuhn versus Lakatos, or paradigms versus research programmes in the history of economics. *History of Political Economy*, *7*(4), 399–433.

Bryant, L., Srnicek, N., & Harman, G. (Eds.). (2011). *The speculative turn: Continental materialism and realism*. Melbourne: re. press.

Buchanan, B. (2017). *The Cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford: Oxford University Press.

Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *IEEE: Proceedings of the VDE Kongress* (Vol. 116, pp. 213–218). Berlin: IEEE.

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96–121.

Dreyfus, H. L. (2008). *On the Internet*. London: Routledge.

Francis, G. (2012). The psychology of replication and replication in psychology. *Perspectives on Psychological Science*, *7*(6), 585–594.

Fuller, S. (2004). *Kuhn vs. Popper: The struggle for the soul of science*. New York, NY: Columbia University Press.

Galloway, A. R., & Thacker, E. (2007). *The exploit: A theory of networks* (Vol. 21). Minneapolis, MN: University of Minnesota Press.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298–303.

Guitton, C., & Korzak, E. (2013). The sophistication criterion for attribution: Identifying the perpetrators of cyber-attacks. *The RUSI Journal*, *158*(4), 62–68.

Habermas, J. (1987). *The philosophical discourse of modernity*. Cambridge: Polity Press.

Hacking, I. (1999). *The social construction of what?* Cambridge, MA: Harvard University Press.

Hutchins, E. (1995). *Cognition in the wild*. Cambridge, MA: MIT Press.

Jackson, P. T. (2008). Foregrounding ontology: Dualism, monism, and IR theory. *Review of International Studies*, *34*(1), 129–153.

Jackson, P. T., & Nexon, D. H. (2013). International theory in a post-paradigmatic era: From substantive wagers to scientific ontologies. *European Journal of International Relations*, *19*(3), 543–565.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7–40.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326–343.

Knake, R. K. (2010). *Internet governance in an age of cyber insecurity* (No. 56). Washington, DC: Council on Foreign Relations.

Kostyuk, N., & Zhukov, Y. M. (2017). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*. doi: 10.1177/0022002717737138

Kuhn, T. S. (1970). Logic of discovery or psychology of research. In I. Lakatos & A. Musgrave (Eds.), *Criticism and the growth of knowledge* (pp. 91–195). Cambridge: Cambridge University Press.

Lakatos, I. (1976). Falsification and the methodology of scientific research programmes. In I. Lakatos & A. Musgrave (Eds.), *Criticism and the growth of knowledge* (pp. 1–24). Cambridge: Cambridge University Press.

Lake, D. A. (2011). Why "isms" are evil: Theory, epistemology, and academic sects as impediments to understanding and progress. *International Studies Quarterly*, *55*(2), 465–480.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.

Layne, C. (1994). Kant or cant: The myth of the democratic peace. *International security*, *19*(2), 5–49.

Lindbekk, T. (1992). The Weberian ideal-type: Development and continuities. *Acta Sociologica*, *35*(4), 285–297.

Mackay, R. (2007). Editorial introduction. *Collapse*, *2*(1), 3–13.

Maxwell, S. E., Lau, M. Y., & Howard, G. S. (2015). Is psychology suffering from a replication crisis? What does "failure to replicate" really mean? *American Psychologist*, *70*(6), 487–498.

Mezzour, G., Carley, K. M., & Carley, L. R. (2015). An empirical study of global malware encounters. In *Proceedings of the 2015 symposium and bootcamp on the science of security*. New York, NY: ACM.

Mindell, D. A. (2002). *Between human and machine: Feedback, control, and computing before cybernetics*. Baltimore, MD: JHU Press.

Mindell, D. A., Segal, J., & Gerovitch, S. (2003). From communications engineering to communications science: Cybernetics and information theory in the United States, France, and the Soviet Union. In M. Walker (Ed.), *Science and ideology: A comparative history* (pp. 66–96). London: Routledge.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs.

Nye, J. S. (2014). *The regime complex for managing global cyber activities*. Cambridge, MA: Harvard Belfer Center.

Phetteplace, E. (2010). Speculative realism. *College & Research Libraries News*, *71*(6), 305–313.

Popper, K. R. (1970). *Normal science and its dangers*. Cambridge: Cambridge University Press.

Radford, B. J. (2016). *Automated learning of event coding dictionaries for novel domains with an application to cyberspace*. (Doctoral dissertation). Duke University, Durham, NC.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1/2), 4–37.

Risse-Kappen, T. (1995). Democratic peace—Warlike democracies? A social constructivist interpretation of the liberal argument. *European Journal of International Relations*, *1*(4), 491–517.

Rosato, S. (2003). The flawed logic of democratic peace theory. *American Political Science Review*, *97*(4), 585–602.

Sat, D. M., Krylov, G. O., Evgenyevich, K., Kasatkin, A. B., & Kornev, I. A. (2016). Investigation of money laundering methods through cryptocurrency. *Journal of Theoretical and Applied Information Technology*, *83*(2), 244–254.

Sgouras, K. I., Birda, A. D., & Labridis, D. P. (2014). Cyber attack impact on critical smart grid infrastructures. In *Innovative smart grid technologies conference (ISGT), 2014 IEEE PES* (pp. 1–5). New York, NY: IEEE.

Shaviro, S. (2003). *Connected: Or what it means to live in the network society*. Minneapolis, MN: University of Minnesota Press.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. London: Penguin.

Sil, R., & Katzenstein, P. J. (2010). Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions. *Perspectives on Politics*, *8*(2), 411–431.

Sowell, J. H. (2012). *Empirical studies of bottom-up Internet governance*. Cambridge, MA: MIT.

Stevens, T. (2017). Cyberweapons: Power and the governance of the invisible. *International Politics*. doi:10.1057/s41311-017-0088-y

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York, NY: Oxford University Press.

Weber, M. (1904). Die "Objektivität" sozialwissenschaftlicher und sozialpolitischer Erkenntnis. [The "objectivity" of socio-scientific and socio-political knowledge]. *Archiv für Sozialwissenschaft und Sozialpolitik*, *19*(1), 22–87.

Weber, M. (2017). *Methodology of social sciences*. London: Routledge.

Wiener, N. (1961). *Cybernetics or control and communication in the animal and the machine* (Vol. 25). Cambridge, MA: MIT Press.

Wiener, N. (1988). *The human use of human beings: Cybernetics and society*. New York, NY: Perseus Books Group.

Yang, G. (2009). *The power of the Internet in China: Citizen activism online*. New York, NY: Columbia University Press.

About the Author

Christopher Whyte is an Assistant Professor in Homeland Security & Emergency Preparedness at the L. Douglas Wilder School of Government & Public Affairs at Virginia Commonwealth University. He teaches coursework on cyber security policy, conflict and law, and has broadly taught coursework on international security topics, political risk analysis and strategic planning. His research interests include a range of international security topics related to the use of information technology in war and peace, political communication and cybersecurity doctrine/policy.