Cyber Conflict in Political Science: A Review of Methods and Literature

Robert Gorwa
Department of Politics and International Relations
University of Oxford
robert.gorwa@politics.ox.ac.uk

Max Smeets
Center for International Security and Cooperation
Stanford University
MwSmeets@Stanford.edu

Draft Paper Prepared for the 2019 ISA Annual Convention

Please do not share without permission

Toronto, March 2019

Abstract

As cyber operations have become a central aspect of modern espionage and intelligence gathering, and now appear to serve as an important element of contemporary foreign policy, political scientists are increasingly publishing work on cyber conflict. However, this literature remains somewhat nascent, and has yet to fully tap into the potential methodological insights of political science. In this paper, we seek to systematically review all cyber conflict articles published in a top-100 political science journal between 1990-2018. We perform a bibliometric analysis, identifying key articles and thematic topics. We also perform a methodological review in an effort to understand the most widely used methods, approaches, and case studies deployed in the lieterature. The findings suggest that the field has perhaps focused on theoretical work at the expense of empirical work, and that cyber conflict scholarship has yet to fully draw upon the broader debates on case selection, case study research, and quantitative/qualitative work that have taken place in political methodology in the last two decades. We briefly conclude with potential future avenues of research that could help amend these challenges.

1. Introduction

As cyber operations have become a central aspect of modern espionage and intelligence gathering, and now appear to serve as an important element of contemporary foreign policy, studies on cyber conflict are increasingly appearing in Political Science and International Relations journals.

The purpose of this study is to systematically review the articles published in these journals. In a *Strategic Studies Quarterly* article, Joseph Nye Jr. wrote in 2011 that "In comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy."[1] A year later, Adam Liff wrote in *the Journal of Strategic Studies* that, whereas for the nuclear domain, scholars like Bernard Brodie have highlighted the implications of nuclear weapons on state interaction, "[n]o comparable comprehensive assessment of the impact of cyberwarfare capabilities exists. Outside the slowly emerging policy literature there is limited scholarly work on the topic, leaving important theoretical questions unexamined".[2] In 2013, Lucas Kello wrote in *International Security*: "The range of conceivable cyber conflict is poorly understood by scholars and decisionmakers, and it is unclear how conventional security mechanisms, such as deterrence and collective defense, apply to this phenomenon. […] [T]here is an evident need for scholars of international relations and security to contribute to the theoretical evaluation of the cyber revolution. Removed from the pressures of having to defeat the cyber threat, yet possessing concepts necessary to analyze it, academics are in a privileged position to resolve its strategic problems. Yet there has been little systematic

[1] Joseph S. Nye, Jr., 2011. Nuclear Lessons for Cyber Security? Strategic Studies Quarterly 5(4): 18-38.
[2] Adam Liff, Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War, The Journal of Strategic Studies Vol. 35, No. 3, 401–428, June 2012

theoretical or empirical analysis of the cyber issue from the perspective of international security."[3]

To what degree is this (still) the case? Is the field now at a higher level of theoretical and analytical maturity? While this has been the matter of significant debate, far less ink has been spilled about the use of methods and measurement in the cyber conflict field. After collecting a corpus of cyber conflict articles published in political science journals, we perform a preliminary bibliometric analysis of cyber conflict scholarship. We also code articles for their methodological approach, showing that there have been few efforts to explicitly engage in qualitative or quantitative research. Our preliminary survey suggests that cyber conflict scholarship has yet to draw significantly upon the broader debates on case selection, case study research, and quantitative/qualitative work that have taken place in political methodology in the last two decades. Through this analysis, we hope to review some of the important work done thus far, and help identify some of the next steps that can help to take the field forward in the future.

We have set up this paper in two parts.[4] Section II presents general bibliometric findings, and the results of our thematic coding. Section III presents the methods-related findings. The final section concludes.

1.2 Research Design

This paper looks at the body of cyber conflict research that has been published in the top Political Science and International Relations (IR) journals.[5] We used the SCImago journal rankings to select the top 100 journals in the field. The ranking is based on a

[3] Kello, "The Meaning of the Cyber Revolution", p.7-8

[4] Readon and Choucri have previously conducted a similar review of the literature on cyberspace. Our review differs in scope in a number of ways: i) we narrowed our review to only cyber conflict research, ii) we focus on a larger set of articles (top 100 journals instead of 20 journals), iii) and include articles from a longer time period. Also, whereas Readon and Choucri only assess the theoretical debates in the literature, this paper also focuses on the methodological approaches of the cyber conflict articles published in political science and IR journals. See: Robert Reardon and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature" Prepared for the ISA Annual Convention San Diego, CA, April 1, 2012.

[5] This means that books on cyber conflict were excluded from this review.

widely used size-independent indicator of scientific journal prestige (SJR2 indicator).[6] A higher index score means that that the portion of prestige is great than that of citable documents, and vice versa.[7]

The search focused on all the journal articles published since January 1980 - January 2019, mentioning on of the following terms in the title or abstract: 'cyber conflict', 'cyber war', 'offensive cyber', 'offensive cyber operations', 'military cyber operations', 'cyber weapons', and 'cyberweapons'. We subsequently used the following selection criteria: (i) articles that were of typical journal-length (e.g. very short articles of 3 or 4 pages were excluded); (ii) articles that primarily focused on cyber conflict issues; iii) and articles that concentrated largely on political science or international relations issues; (iv) articles that were stand alone articles, and not the editorial introductions for a special issue.[8] Of those 149 articles, 70 matched our topic-specific selection criteria (as centrally about cyber-conflict, as opposed to nuclear or terrorism related issues). For example, this meant that articles tackling the radicalization of ISIS fighters on the internet were excluded from our final analysis. (The complete list of articles can be found in Appendix I.)

2. General Overview and Bibliometrics

149 articles that met our initial keyword-based search criteria. The articles were sorted according to year, topic, and journal, and analyzed using the R package 'bibliometrix.'[9] Articles from 19 different journals were included in the dataset. As seen in *Figure 1*, the journals with the most articles include the *Journal of Strategic Studies*, *Survival*, and the *Journal of Cybersecurity*.

[6] For a description see Vicente P. Guerrero-Bote and Félix Moya-Anegón, "A further step forward in measuring journals' scientific prestige: The SJR2 indicator," *Journal of Informetrics*, 6 (2012) 674–688
[7] ibid; We made one exception, as we also included the *Journal of Cybersecurity*, given that it is a relatively new and influential journal in the field.
[8] This coding was done manually. No automated techniques were required given the small sample.
[9] Massimo Aria and Corrado Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *Journal of Informetrics*, 11 (2017), 959-975.

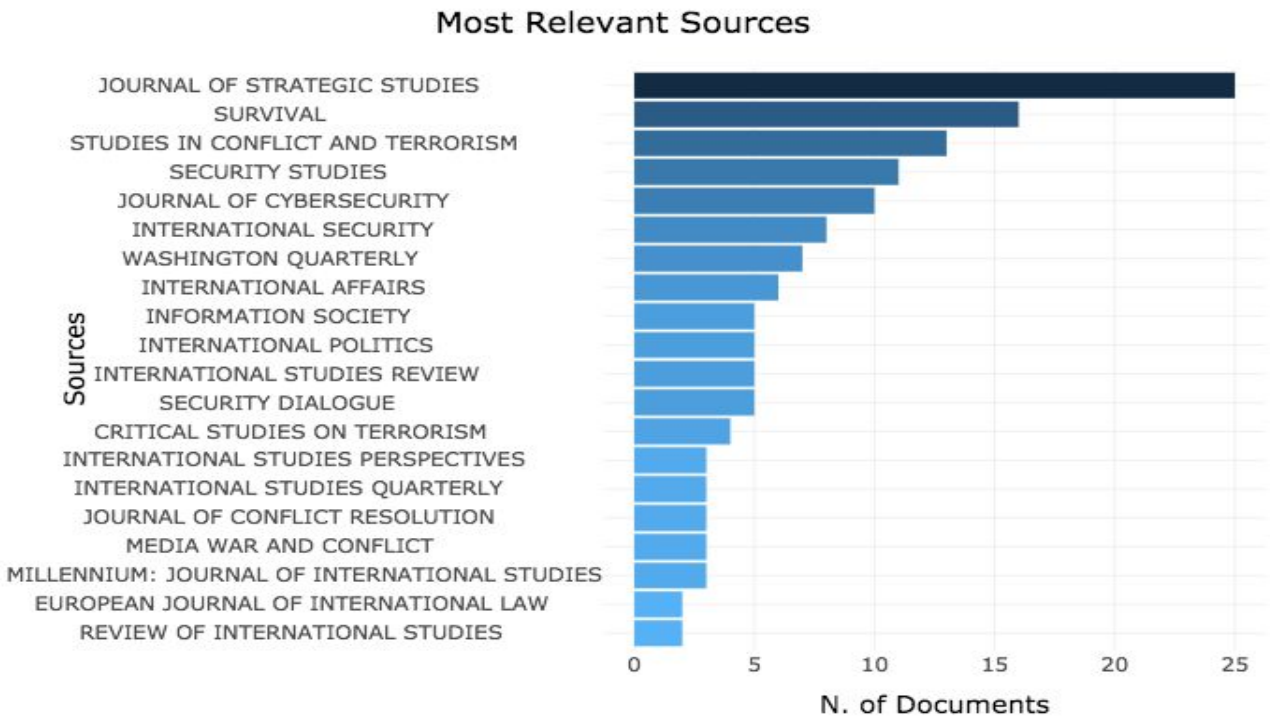

Fig. 1: Top journals in corpus

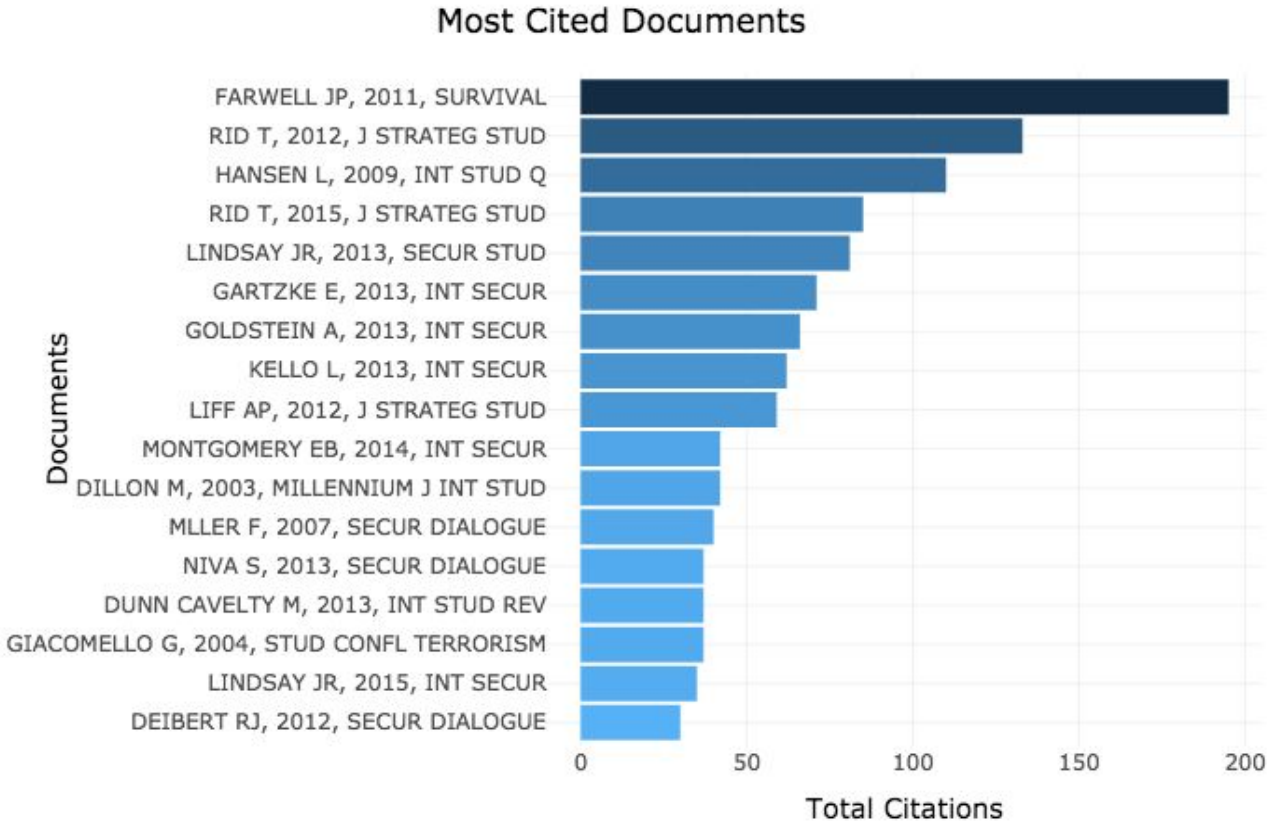

Fig. 2: Most Cited Journals (Scopus)Fig. 2: Most Cited Journals (Scopus)

Jason Healey identifies three phases of cyber conflict history: realization (1980s), takeoff (1990s-), and militarization (2003-).[10] While the academic cyber conflict literature is over two decades old, as *Figure 3* indicates, it is only after 2010 that a significant number of cyber conflict articles were published in the top political science journals.[11] In other words, comparing the policy and academic 'timelines', it took some time before the (American) political science literature caught up to developments in the policy-community and started to analyze issues of cyber conflict in a more rigorous manner. Yet, cyber conflict remains to be a relatively small field within Political Science. This is also shown in the number of citations per article. The articles with the most citations, according to Scopus, include Farwell and Rohozinski's *Stuxnet and the Future of Cyber War* (186), Rid's *Cyber War Will Not Take Place* (130), Hansen and Nissenbaum *Digital Disaster, Cyber Security, and the Copenhagen School* (109), and Rid and Buchanan's *Attributing Cyber Attacks* (81).[12] Even compared to other emerging fields within Political Science (such as climate politics and governance), cyber conflict articles appear to be relatively less cited.[13]

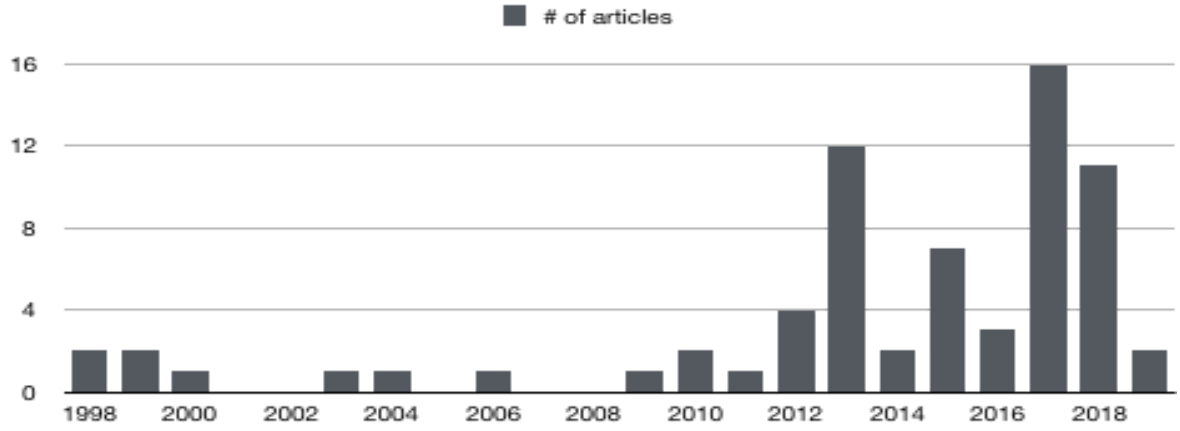

Fig. 3: Number of articles in final dataset, by year (n = 70)

[10] Jason Healey (ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* (Vienna, VA: Cyber Conflict Studies Association, 2013)
[11] The figure can be misleading as special issues can greatly distort the aggregate numbers.
[12] Note that this is based off of Scopus citation data, which focuses only on academic sources and is more restrictive than Google Scholar (which also included online pre-prints, reports, and policy documents). For an overview of how the Google Scholar Citations metric works see: https://scholar.google.com/intl/en/scholar/about.html
[13] The majority of articles had less than 10 citations.

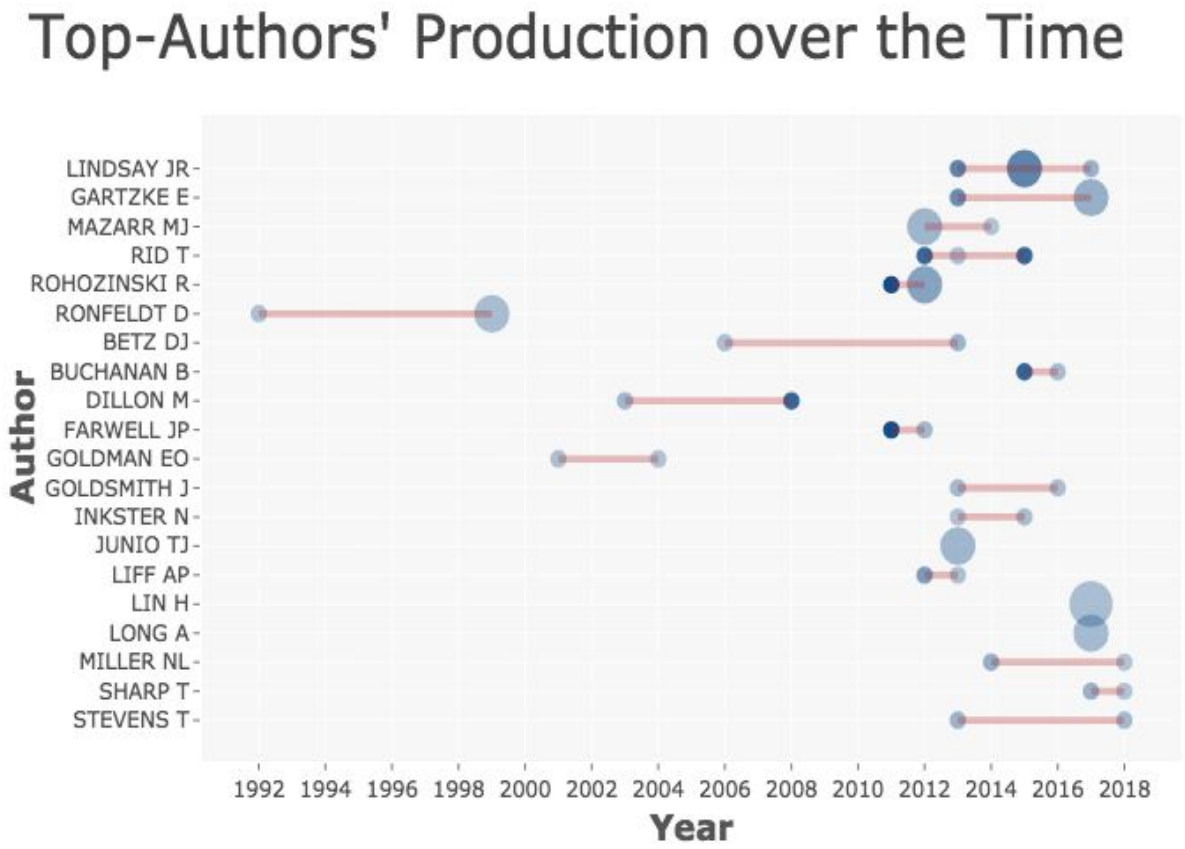

Fig. 4: Top authors in corpus. Each dot is an article, larger dots represent multiple articles in one year. The darker the dot, the more citations it has. E.g. Herb Lin has three articles in 2017 in our corpus; Jon Lindsay published one in 2013, two in 2015, and one in 2017.

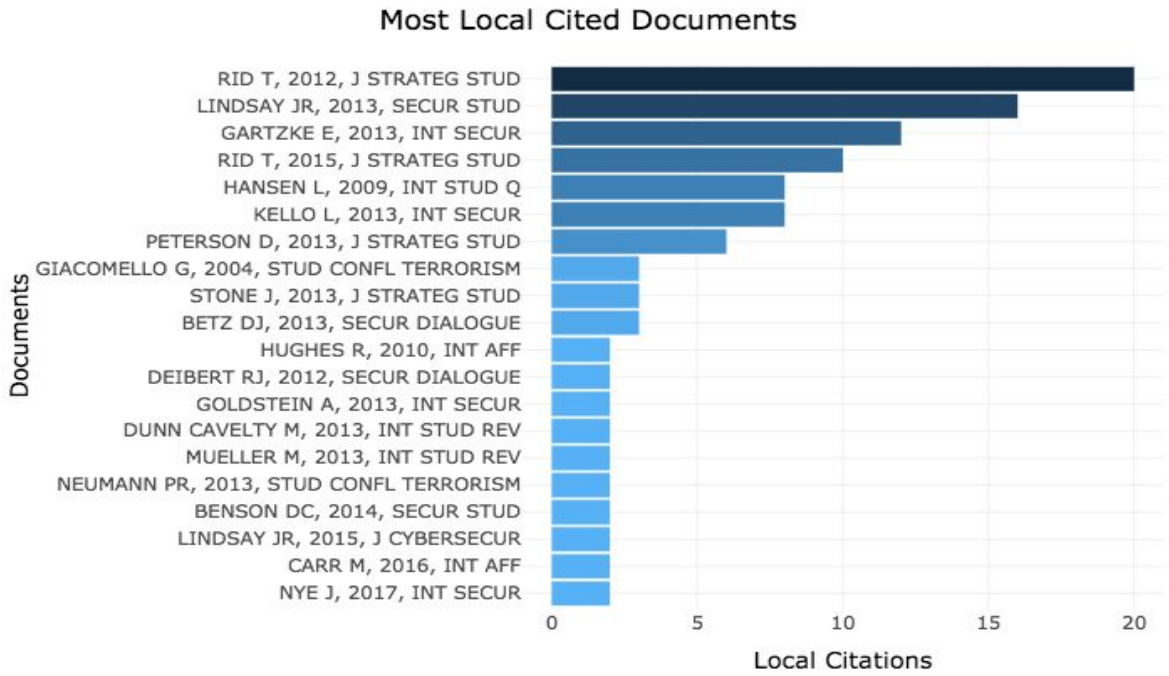

Fig. 5: Articles cited the most by articles in our dataset

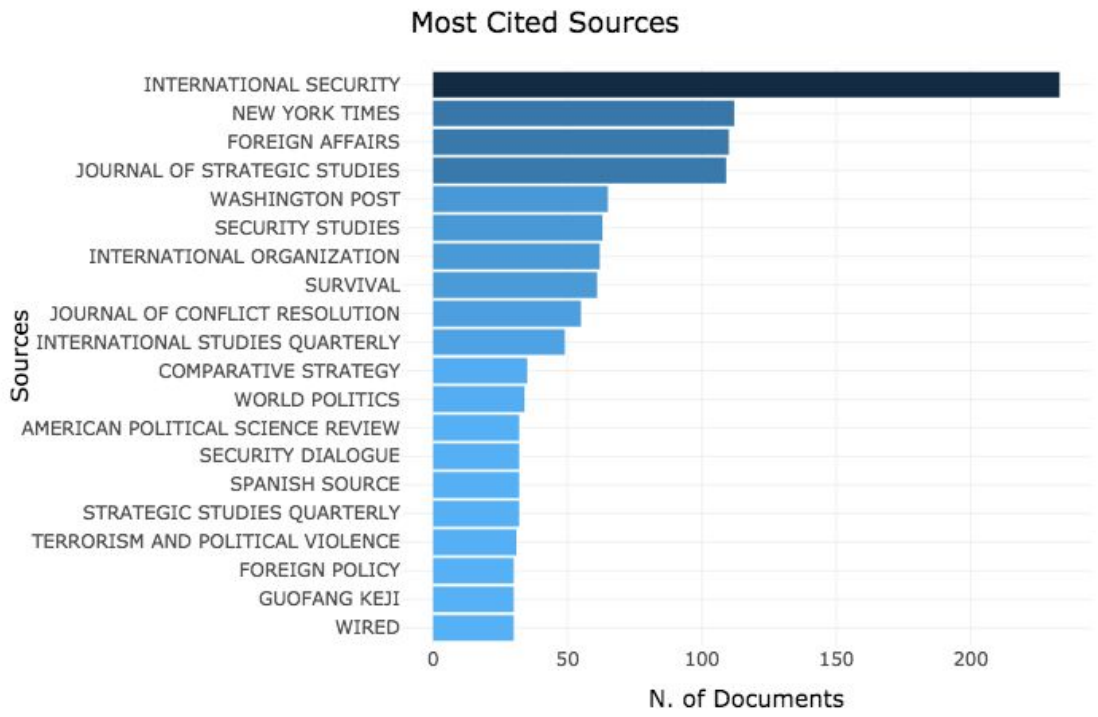

Fig. 6: Most cited sources (journals, newspapers) by articles in our corpus

The bibliometrix package allows one to analyze a large set of bibliographies, based on Scopus and Web of Science indexing. *Figure 5* demonstrates the articles that were the most cited by the 70 articles in our dataset. *Figure 6* outlines the top sources that were cited (e.g. journals, newspapers, reports) by articles in our dataset. It is notable that articles in *International Security* appear to be highly influential and widely, despite their relative scarcity in our corpus (only 6 articles, although this figure would include non-cyber *IS* references as well). As well, the *New York Times* and *Washington Post* feature very strongly (demonstrating the cyber conflict literature's frequent engagement with journalism and reporting on incidents).

2.2 Subject Overview

What are the major themes and topics in our corpus? We non-exclusively coded the articles based on issue area,[14] meaning that articles can address more than issue.

[14] Readon and Choucri sorted the articles based on particular theoretical paradigm. We decided to not follow the same approach as most articles do not fall within a clear theoretical paradigm

Figure 5 provides a detailed overview of issues addressed, distinguishing between three periods: the early literature from 1995 to 2009, the second period literature from 2010-2015, and the more recent literature published since 2016.[15] These themes were coded inductively by the two authors — future versions of the paper could involve more coders and inter-coder reliability.

While discussing every topic in depth goes beyond the scope of this article, it is worth discussing the key issue areas in more detail. Our analysis suggests that, many topics, such as proliferation and attribution, widely considered key themes in the literature, have not really received lengthy, repeated attention.[16]

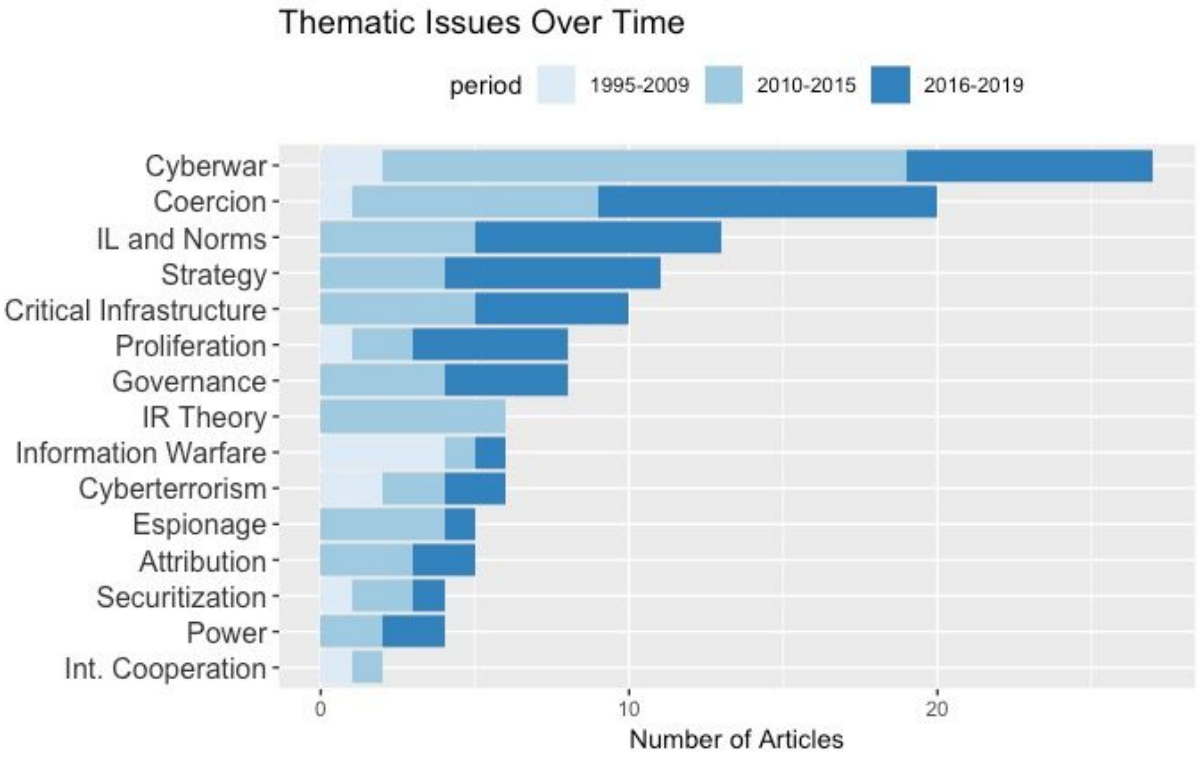

Fig. 5: Cyber Conflict coded for topics across three time periods, per issue area

[15] This breakdown was based on the findings shown in Figure 1. It was evident that there was a significant increase in articles since 2010.
[16] Also see: Max Smeets (2018) A matter of time: On the transitory nature of cyberweapons, *Journal of Strategic Studies*, 41:1-2, 6-32,

First, the discussion of cyber war has dominated the literature over the past decade. To understand the emergence of this literature, however, we have to look beyond the publications in the top 100 Political Science and IR journals. John Arquilla and David Ronfeldt wrote as early as 1993 about the coming of cyberwar, explaining how information and and communication infrastructure can be disrupted during military conflicts.[17] That said, much of the early literature discussed "netwar" or "information war," as we can see from the relatively few 'cyberwar' articles in our dataset that were published before 2009.

Betz and Stevens have noted that the "[p]opular discourse on cyberwar tends to focus on the vulnerability of the 'physical layer' of cyberspace to cyber-attack and the ways in which this may permit even strong powers to be brought to their knees by weaker ones, perhaps bloodlessly."[18] Clarke and Knake wrote one of the most widely read books on "cyberwar" in 2010, and helped spur a significant increase in academic articles discussing the concept. Whereas some scholars believe cyberwar is 'inevitable', others are more skeptical — observing a striking absence of cyber attacks above the threshold of armed attack.[19] In our dataset of academic articles, 2010-2015 appears to be the golden age of 'cyberwar' scholarship, including Thomas Rid's eventual article (and book) that sought to push back against the cyberwar hype.[20] These more critical scholars appear to have been to some degree successful, as the term appears to have fallen out of favour since 2016.

---

[17] John Arquilla and David Ronfeldt, "Cyberwar is coming!," *Comparative Strategy*, 12:2 (1993)141-165; also see John Arquilla and David Ronfeldt, "In Athena's Camp: Preparing for Conflict in the Information Age", (Santa Monica: The Rand Corporation); John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, (Santa Monica: Rand Corporation: 2001).

[18] David J. Betz and Tim Stevens, "Cyberspace and the State: Towards a Strategy for Cyber-Power," Adelphi Series , 51:424 (2011)75-98, p.76

[19] Thomas Rid, "Cyber War Will Not Take Place." *Journal of Strategic Studies,* 35:1 (2012): 5-32; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security,* 38: 2 (2013): 41–73; Adam P. Liff, " Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, 35:3 (2012)401-428

[20] Rid, Cyber war will not take place.

Second, as numerous national strategies talk about the increasing role of offensive cyber operations, it is hardly surprising that coercion — understood here following Schelling as deterrence and compellence -- has received a great deal of attention in the literature.[21] Whereas there are few works on compellence,[22] a large number of articles in our corpus discuss how cyberattacks can be deterred by an adversary through the (threatened) use of a broad set of means.[23] Many of the published articles in our corpus argue that that whilst it is more difficult to deter cyberattacks, there are ways policymakers can dissuade actors from attacking.[24] For example, Uri Tor proposes the notion of cumulative cyber deterrence: we should not seek to deter individual attacks but a series of attacks.[25]

Third, global rules or norms of state behavior to minimize the impact of cyber proliferation have been proposed since the late 1990s. More concrete discussions have take place since 2004, when the United Nations Secretary General first appointed a group of governmental experts (UNGGE) on 'Developments in the Field of Information and Telecommunications in the Context of International Security'.[26] However, our dataset only had articles that explore international law and international norms post-2010, as the Tallinn Manual process began in 2009, and these topics have been only covered increasingly in our sampled journals in the past decade.

---

[21] Following Shelling, coercion in this context refers to both deterrence and compellence. Thomas Shelling, *Arms and Influence*, (Yale University Press: 1966)

[22] Borghard and Lonergan, The Logic of Coercion in Cyberspace

[23] Cyber deterrence can have at least two different meanings, often conflated. First, cyber deterrence can refer to the use of a cyber capability to deter a certain type of (military) means of an adversary. Second, cyber deterrence can refer to how a broad set of means can deter a cyber attack of an adversary. This article focuses on the latter. See: Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?" 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, T. Minárik, R. Jakschis, L. Lindström (Eds.) (Tallinn: NATO CCD COE Publications: 2018)

[24] Jon R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," 1: 1 (2015) 53–67

[25] Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies*, 40:1-2(2017)92-117

[26] Also see: Joseph Nye Jr. "https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf

There are many other interesting trends that could be discussed in our presentation, including that the strain of literature on applying IR theory to cyber conflict issues may have dried up (no articles since 2016), or that the literature on military and state strategy as it pertains to cyber conflict appears to have increased significantly in the top 100 political science journals in the past three years.

3. Methods Overview

What are the major methodological approaches, methods, and methodological challenges in the cyber conflict literature? Cyber conflict articles published in political science journals differ in goal, scope and theoretical approach. This can make it difficult to compare the use of methodology across the literature. That said, we sought to better understand the methodological state of the field as well as we could despite the inherent limitations. We coded our dataset of articles on a number of categories, which we discuss in this section.

Research Design

Only 9 articles explicitly discuss use of methods and/or have a separate research design section.[27] Articles that have a research design tend to be the ones that collect or use empirical data (also 9/70 articles). One reason why many of the articles lack an explicit research design is because of the type of journal they are published in: the *Journal of Strategic Studies* and *Survival* - two journals strongly represented in our dataset - are theoretical and policy oriented rather than empirical journals.

Theory-building vs. Theory-testing

Political Science literature is often divided into theory building and theory testing studies.[28] As coded in our dataset, most cyber conflict articles (39) appear to be theory

[27] We do not make an explicit distinction between research design section and methods section
[28] A similar distinction can be made between research that focuses on hypothesis-generating versus hypothesis-testing.

building articles — in the broad sense the articles seek to provide new explanations for a cyber conflict phenomenon through novel theoretical understanding or describing a causal mechanism. Only 17 articles at least partially sought to find evidence to confirm or refute a theory. Furthermore, 14 articles were descriptive in nature - not seeking to test nor construct a theoretical framework or causal mechanism, but rather to describe an operation, campaign, or state of affairs.

The strong focus on theory-building, rather than testing, could be due to at least two reasons. The first is that cyber conflict is still a young field. Also, many experts believe that the dynamics of cyber conflict are substantially different from conventional conflict. This means that new, theoretical research is required to understand and explain these different dynamics. Only after this path-breaking research is conducted, we can turn to the task of trying to verify or falsify these theories through empirical research. In Gerring's words, we are still at the 'lightbulb' moment and have not yet moved to the 'skeptical' moment. (It's important to qualify this argument and note that it was difficult for us to distinguish between theory-building and testing in many of these cases, perhaps because many articles did not explicitly set out their aims along those lines).

Another often-cited reason concerns the lack of empirical data. The secrecy surrounding government organizations and their capabilities as well as the anonymity of attackers complicates theory-testing research. Much of the data and reporting on cyber operations comes from from cyber security firms, such as *McAfee*, *Symantec*, *Kaspersky*, *Crowdstrike*, *Fox-IT*, and *Arbor*. The problem is that much of the (public) reporting by these firms is done for marketing reasons and remains political: indeed, few have reported on western operations (especially US-based firms).[29] Despite this constraint, there is still a vast amount of raw data and other documents that await

[29] It might not be surprising that most Western APTs (such as Equation Group and the Mask) are uncovered by Kaspersky Lab. For an overview see: APT Groups and Operations, https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=361554658

further analysis.[30] As one participant observed at the State of the Field Workshop on Cyber Conflict 2017: there is still "a lot of low-hanging fruit remains when it comes to data gathering and analysis. There is still much more to be done in terms of coding these events."[31]

Causality & quantitative vs qualitative

To better understand the nature of cyber conflict research, it is worth placing the research in Henry Brady's causality framework.[32] Brady discusses four approaches to causality in Political Science. First, there is the approach of *Neo-Humean regularity* - going back to Hume and Mill, which seeks to determine causality through the "observation of constant conjunction and correlation" and "temporal precedence".[33] Second, there is the *counterfactual* approach, addressing causality through understanding truth in otherwise similar worlds of "if the cause occurs then so does the effect" and "if the effect does not occur, then the cause may still occur."[34] Third, there is the *manipulation* approach, seeking to determine a "recipe that regularly produces the effect from the cause" and an "observation of the effect of manipulation."[35] Finally, there is the *mechanisms and capacities* approach, focusing on the operation of the mechanism or capacity that leads from the cause to the effect.

The vast majority of cyber conflict articles focus on the latter form of causality. The main cause of effect described in the literature is the *nature* of cyberspace or cyber operations. For example, it is commonly said that, the lack of (clear) borders and the interconnectedness of computer systems and networks makes cyber deterrence more

[30] Also see: Max Smeets & Jason Healey, "Cyber Conflict History", 2017 State of the Field of Cyber Conflict Workshop Columbia University School of International and Public Affairs; for a similar discussion see: Kello, "The Meaning of the Cyber Revolution"
[31] Ibid
[32]Henry E. Brady, "Causation and Explanation in Social Science," in The Oxford Handbook of Political Methodology, Janet M. Box-Steffensmeier, Henry E. Brady, and David Collier, editors, p. 8
[33] Ibid.
[34] Ibid.
[35] Ibid.

difficult. Similar variables are cited in relation to collateral damage and other issues,[36] such as the common notion that low barriers of entry create a diffusion of cyber-power, [37] or that the “invisible" nature of “cyber weapons” makes it difficult to govern and set up arms control treaties.[38] Few articles—if any—focus on how organizational structure or individual perception causes certain outcomes in cyber conflict.

Just six articles deploy a research design that suits the other three approaches of causality (large N studies for *Neo-Humean approach* and experiments for the *counterfactual* and *manipulation* approach). Of these, two create an event-based dataset. This includes the work of Valeriano and Manness on “The dynamics of cyber conflict between rival antagonists” and Kostyuk and Zhukov on how cyber attacks may shape battlefield events. Two others are experimental studies of cyber terrorism and one is a survey of cyberterrorism researchers.[39] Cyberterrorism research, suffering from an extreme paucity of cases, has been creative in deploying thought experiments and other types of simulation designs. Finally, Lindsay’s study *on* “the attribution problem and the feasibility of deterrence against cyberattack” is the only article that appeared in our dataset that deployed a formal model to describe a dynamic of cyber conflict. The formal model seeks to demonstrate “how different assumptions about costs and uncertainty affect the coverage and effectiveness of deterrence by denial and punishment.”

While we coded the other articles as ‘qualitative’, only two articles explicitly claimed that they engaged in qualitative research. These included Christensen and Petersen’s exploration of public-private security partnerships, and Kostyuk and Zhukov’s research

[36] see: Bellovin, Lin and Landau, “Limiting the undesired impact of cyber weapons: Technical requirements and policy implications”
[37] See for example: Betz, “Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed”
[38] See for example: Hughes, “A treaty for cyberspace”; Stevens, “Cyberweapons: Power and the governance of the invisible”
[39] Gross, Canetti, Vashdi, “Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes”; Armenia and Tsaples, "Individual behavior as a defense in the “war on cyberterror”: A system dynamics approach”. Jarvis, Macdonald, Nouri, “The Cyberterrorism Threat: Findings from a Survey of Researchers”

into local conflict in Ukraine, both of which deployed approximately 20 qualitative interviews (in the case of Kostyuk and Zhukov, to triangulate quantitative findings as part of a mixed-methods research design). A handful of articles utilized interviews as an extra resource, citing them to bolster their argument. (For instance, Slayton uses one interview, Rid and Buchanan's work on attribution draws on a few interviews and a focus group, and Nocetti conducts some interviews with internet governance specialists). However, these interviews are supplementary, used to provide additional background source material, rather than as part of a qualitative research design. None of the three articles discuss the pros and cons of qualitative research, cite the ample literature on interviewing in political science, or even describe how many interviews they conducted.

3.1 A Closer Look at Qualitative Research

In his classic work, Gerring defines as a case study as "the intensive study of a single case where the purpose of that study is – at least in part – to shed light on a larger class of cases (a population)." He also notes that "[c]ase study research may incorporate several cases, that is, multiple case studies. However, at a certain point it will no longer be possible to investigate those cases intensively. At the point where the emphasis of a study shifts from the individual case to a sample of cases, we shall say that a study is cross-case. Evidently, the distinction between case study and cross-case study is a matter of degree. […] All empirical work may be classified as either case study (comprising one or a few cases) or cross-case study (comprising many cases)."[40]

Cyber conflict case study research tends to focus on a small set of cases.[41] Four events received the most attention in our dataset: Estonia, Georgia, Stuxnet, and the

[40] John Gerring, *Case Study Research: Principles and Practices*, p. 20

[41] Most single case or cross-case studies focused on events or operations (11). We also coded five articles as deploying country level case studies. These distinctions, however, are not always clear. For example, Hansen and Nissenbaum's securitization research analyzes the discourse in Estonia following the Estonian DDoS attacks, blurring the lines between the two.

Sony hack, with a few articles performing detailed case studies into a single event.[42] There are distinct types of case studies: typical, diverse, extreme, deviant, influential, crucial, pathway, most-similar, and most-different. Case study selection is important to better understand the generalizability of the findings. However, we found that case study selection is rarely justified in the cyber conflict articles that use case studies. Out of the 16 articles we coded as deploying case studies, 7 justified their selection in some way. Only Kostyuk and Zhukov's article justified their case selection using methodological literature from political science, indicating that they were selecting two most-likely cases.[43]

Another article that stands out for its case-study analysis is an article from Efrony and Shany, exploring the "Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." As the article seeks to evaluate states' acceptance of the rules in the Tallinn Manual, the authors selected 11 cases, each described in substantial detail, through a multistage-stage process for case selection.[44] They set up five inclusion and exclusion criteria based on the research foci, asked a third-party search firm to conducted an extensive web-crawl for cyberoperations, and compared that list of cases with the datasets from Center for Security and Intelligence Studies' (CSIS) "list of incidents," and the U.S. Council on Foreign Relations' (CFR) Cyber Operations Tracker. Finally, the case studies were grouped into six categories, according to the identity of the victim state—a categorization that helped the authors to establish the consistent practice of such states.

[42] For three prominent *single* case study events on Stuxnet in the Corpus see: Lindsay, "Stuxnet and the Limits of Cyber Warfare"; Farwell and Rohozinski, "Stuxnet and the future of cyber war"; Slayton, "What is the cyber offense-defense balance? Conceptions, causes, and assessment" (in all other top 20 articles, published after 2011, Stuxnet was cited as a (key) example as well.

[43] Those (theory-testing) studies which are not explicit about their case-selection have a strong tendency to select most-likely rather than least-likely cases (and discuss these cases to confirm their theory).

[44] Efrony and Shany, "Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", p. 594-596

The most common approach in our dataset was to simply marshal examples support their argument. Rather than engaging with a handful of in-depth case studies, these articles weave historical examples (and primary and secondary source material that included government reports, reports published by threat intelligence companies, and news coverage) into their argument. This is of course understandable when there is a relatively limited number of well-known cases that are widely acknowledged as important; however, this approach is not systematic, and cases can easily be cherry picked to fit the argument that is being deployed.

3.2 A Closer Look at Quantitative Research

There were only two quantitative articles that sought to understand conflict dynamics at the international or sub-national level. Valeriano and Maness did a lot of legwork to create the first dyadic county-level dataset, which aims to capture all cyber incidents and disputes between rival states for the years 2001-2011.[45] Valeriano and Maness look at "[c]yber engagements directed by one state against another" in order to "determine which rival states have been using cyber tactics and where these attacks are directed".[46] Kostyuk and Zhukov's work seeks to correlate the incidence of cyber attacks with local conflict dynamics and fighting on the ground.

The work raises several issue areas that researchers should consider if they want to further this field of quantitative research. A problem with coding a dyadic-country level dataset is that most malware affects a large amount of systems in a large amount of countries. How many systems should get infected in a country for it to be included as a dyad? Or what level of harm or damage should be caused? Equally, it likely leads to an over-representation of worms and virus and an underrepresentation of DDoS-attacks in the dataset due to the targeted nature.

[45] Valeriano, and Maness, "The dynamics of cyber conflict between rival antagonists, 2001-2011"
[46] Ibid, p. 347

Another problem with coding a dyadic-country level dataset concerns the lack of data on attribution. In most cases, there is little attribution info available - ie. we not entirely sure about the country of origin, but above all we are not sure if it was a non-state or state actor conducting the attack. Also, many groups have multinational membership. For example, the Pakistan Cyber Army and the Muslim Liberation Army have numerous members in Saudi-Arabia, the United States and Europe.

Third, it is often hard to assess which country is the target/victim of a cyber attack. Consider for example the case of Iran infiltrating the computer networks of Dutch company Diginotar to retrieve digital certificates to spy on Iranian citizens. Similarly, with the recent US strategy of 'Defend Forward,' we could feasibly imagine a case of the US disrupting a Russian operation in 'gray space' — such as network servers in Nairobi or routers in a different country. It is not immediately clear how these type of cases should be coded in a dyadic manner. Kostyuk and Zhukov's quantitative modelling is sophisticated, but suffers from data issues: the paper hinges on the accurate identification of Ukranian "cyber attacks," and draws from a private firm's 'Digital Attack Map' that seeks to track network disruptions and DDoS attacks.

These problems help illustrate why there has been so little quantitative research in the field. However, they should not preclude future work, which could fruitfully explore a number of issue areas, such as, for instance, the unequal reliance on cyber proxies by states. Although there seems to be a general consensus in the sparse literature that states use cyber proxies as a vehicle because they can plausibly deny a relationship — Maurer notably states that "a general political incentive for states to use proxies is summed up by the concept of 'plausible deniability"[47] — that argument creates a puzzle. Based on the plausible deniability argument, we should expect democracies, as states with high levels of public accountability and greater attentiveness to reputational costs than authoritarian regimes, to primarily rely on these types of actors.

[47] Maurer, "Cyber proxies and their implications for liberal democracies"

Yet, we observe the reverse pattern: it seems to be states like Russia and Iran that primarily act through cyber proxies. Why? Perhaps the availability and cost-effectiveness of using non-state actors plays as a role, as well as many other possible factors. Quantitative research could help us better explain the dynamics of this relationship, and help explore other outstanding questions for cyber conflict scholars.

4. Conclusions for ISA

This remains very much a work in progress. We know that there could be two different, interconnected papers here: a bibliometric analysis comprehensive mapping of the literature, as well as the second piece concerned with methods and methodology. As seen here, we sought to bring out the second in as systematic a manner as possible, creating a (hopefully) defensible corpus of articles and reviewing them in turn, rather than selecting papers to assess at random.

We would really appreciate general feedback about the project, as well as any specific feedback into either of the two parts of the analysis. What are any questions that you think we should explore further? Are we missing anything here? Are there other key articles that we should include or discuss in more detail? Many thanks for reading!

Appendix 1

The articles found in the search are found in table A1:

Table A1: List of selected articles

Authors	Title	Year	Journal Title
Jacobson M.R.	War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks	1998	Journal of Strategic Studies
Feaver P.D.	Blowback: Information warfare and the dynamics of coercion	1998	Security Studies
Arquilla J., Ronfeldt D.	The advent of netwar: Analytic background	1999	Studies in Conflict and Terrorism
Valeri L., Knights M.	Affecting Trust: Terrorism, Internet and Offensive Information Warfare	2000	Terrorism and Political Violence
Rathmell A.	Controlling computer network operations	2003	Studies in Conflict and Terrorism
Giacomello G.	Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism	2004	Studies in Conflict and Terrorism
Betz D.J.	The more you know, the less you understand: The problem with information warfare	2006	Journal of Strategic Studies
Hansen L., Nissenbaum H.	Digital disaster, cyber security, and the copenhagen school	2009	International Studies Quarterly
Hughes R.	A treaty for cyberspace	2010	International Affairs
Manjikian M.M.	From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik	2010	International Studies Quarterly
Farwell J.P., Rohozinski R.	Stuxnet and the future of cyber war	2011	Survival
Rid T.	Cyber War Will Not Take Place	2012	Journal of Strategic Studies
Liff A.P.	Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War	2012	Journal of Strategic Studies
Betz D.	Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed	2012	Journal of Strategic Studies
Deibert R.J., Rohozinski R., Crete-Nishihata M.	Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war	2012	Security Dialogue
Farwell J.P., Rohozinski R.	The new reality of cyber war	2012	Survival
Goldsmith J.	How cyber changes the laws of war	2013	European Journal of International Law

Gartzke E.	The myth of cyberwar: Bringing war in cyberspace back down to earth	2013	International Security
Kello L.	The meaning of the cyber revolution: Perils to theory and statecraft	2013	International Security
Dunn Cavelty M.	From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse	2013	International Studies Review
Mueller M., Schmidt A., Kuerbis B.	Internet security and networked governance in international relations	2013	International Studies Review
Junio T.J., Mahnken T.G.	Conceiving of future war: The promise of scenario analysis for international relations	2013	International Studies Review
Peterson D.	Offensive Cyber Weapons: Construction, Development, and Employment	2013	Journal of Strategic Studies
Stone J.	Cyber War Will Take Place!	2013	Journal of Strategic Studies
McGraw G.	Cyber War is Inevitable (Unless We Build Security In)	2013	Journal of Strategic Studies
Junio T.J.	How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate	2013	Journal of Strategic Studies
Betz D.J., Stevens T.	Analogical reasoning and cyber security	2013	Security Dialogue
Lindsay J.R.	Stuxnet and the Limits of Cyber Warfare	2013	Security Studies
Valeriano B., Maness R.C.	The dynamics of cyber conflict between rival antagonists, 2001-11	2014	Journal of Peace Research
Jarvis L., Macdonald S., Nouri L.	The Cyberterrorism Threat: Findings from a Survey of Researchers	2014	Studies in Conflict and Terrorism
Nocetti J.	Contest and conquest: Russia and global internet governance	2015	International Affairs
Lindsay J.R.	The impact of China on cybersecurity: Fiction and friction	2015	International Security
Lindsay J.R.	Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack	2015	Journal of Cybersecurity
Rid T., Buchanan B.	Attributing Cyber Attacks	2015	Journal of Strategic Studies
Cornish P.	Governing cyberspace through constructive ambiguity	2015	Survival
Cavaiola L.J., Gompert D.C., Libicki M.	Cyber House Rules: On War, Retaliation and Escalation	2015	Survival
Meyer P.	Seizing the Diplomatic Initiative to Control Cyber Conflict	2015	Washington Quarterly
Stoddart K.	UK cyber security and critical national infrastructure protection	2016	International Affairs
Lupovici A.	The "attribution problem" and the social construction of "violence": Taking cyber deterrence literature a step forward	2016	International Studies Perspectives

Buchanan B.	The life cycles of cyber threats	2016	Survival
Christensen K.K., Petersen K.L.	Public-private partnerships on cyber security: A practice of loyalty	2017	International Affairs
Nye J.S., Jr.	Deterrence and dissuasion in cyberspace	2017	International Security
Slayton R.	What is the cyber offense-defense balance? Conceptions, causes, and assessment	2017	International Security
Gartzke E., Lindsay J.R.	Thermonuclear cyberwar	2017	Journal of Cybersecurity
Gross M.L., Canetti D., Vashdi D.R.	Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes	2017	Journal of Cybersecurity
Bellovin S.M., Landau S., Lin H.S.	Limiting the undesired impact of cyber weapons: Technical requirements and policy implications	2017	Journal of Cybersecurity
Farrell H., Glaser C.L.	The role of effects, saliencies and norms in US Cyberwar doctrine	2017	Journal of Cybersecurity
Libicki M.C.	Second acts in cyberspace	2017	Journal of Cybersecurity
Weber S.	Coercion in cybersecurity: What public health models reveal	2017	Journal of Cybersecurity
Robert Kehler C., Lin H., Sulmeyer M.	Rules of engagement for cyberspace operations: A view from the USA	2017	Journal of Cybersecurity
Long A.	A cyber SIOP? Operational considerations for strategic offensive cyber planning	2017	Journal of Cybersecurity
Tor U.	'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence	2017	Journal of Strategic Studies
Sharp T.	Theorizing cyber coercion: The 2014 North Korean operation against Sony	2017	Journal of Strategic Studies
Borghard E.D., Lonergan S.W.	The Logic of Coercion in Cyberspace	2017	Security Studies
Grigsby A.	The end of cyber norms	2017	Survival
Fischerkeller M.	Incorporating offensive cyber operations into conventional deterrence strategies	2017	Survival
Efrony D., Shany Y.	A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice	2018	American Journal of International Law
Stevens T.	Cyberweapons: Power and the governance of the invisible	2018	International Politics
Ziegler C.E.	International dimensions of electoral processes: Russia, the USA, and the 2016 elections	2018	International Politics
Acton J.M.	Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war	2018	International Security
Smeets M.	A matter of time: On the transitory nature of cyberweapons	2018	Journal of Strategic Studies

Sleat M.	Just cyber war?: Casus belli, information ethics, and the human perspective	2018	Review of International Studies
Armenia S., Tsaples G.	Individual behavior as a defense in the “war on cyberterror”: A system dynamics approach	2018	Studies in Conflict and Terrorism
Sharp T.	Hiding in plain sight: Political effects of cyber operations	2018	Survival
Boeke S., Broeders D.	The demilitarisation of cyber conflict	2018	Survival
Joo Y.-M., Tan T.-B.	Smart cities: A new age of digital insecurity	2018	Survival
Maurer T.	Cyber proxies and their implications for liberal democracies	2018	Washington Quarterly
Kostyuk N., Zhukov Y.M.	Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?	2019	Journal of Conflict Resolution
Wilner A.S.	US cyber deterrence: Practice guiding theory	2019	Journal of Strategic Studies