Article

Journal of Conflict Resolution
2024, Vol. 68(1) 80–107

DOI: 10.1177/00220027231160993
journals.sagepub.com/home/jcr
Sage

Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations

Nadiya Kostyuk[1] and Erik Gartzke[2]

Abstract

Pundits debate whether conflict in cyberspace is more likely to trigger or preempt conflict in other domains. We consider a third possibility. Rather than directly complementing or substituting for traditional forms of conflict, the Internet could separately affect *both* virtual and kinetic dispute behavior. Specifically, we argue that a country's increasing Internet access causes it to engage in aggressive cyberspace behavior more often. At the same time, economic and social changes associated with the information age reduce the utility of pursuing more traditional forms of conflict. Cyberspace offers an attractive domain in which to shape the balance of power, interests, and information in a technological era, while territorial conquest has become somewhat anachronistic. We test our theory using an innovative estimation approach, applied to panel data on cyber versus conventional disputes. Our findings confirm this indirect substitutability between cyber and conventional conflict.

Keywords

(cyber) conflict, complementarity, substitutability, independence, Internet access

[1]School of Public Policy and School of Cybersecurity and Privacy, Georgia Institute of Technology, USA
[2]University of California, San Diego, La Jolla, CA, USA

Corresponding Author:
Nadiya Kostyuk, School of Public Policy and School of Cybersecurity and Privacy, Georgia Institute of Technology, USA.
Email: nkostyuk3@gatech.edu

In recent decades, governments have begun to consider cyberspace as yet another domain in which to pursue political competition. Most of the features of this new domain remain subject to speculation. Nevertheless, it is possible to investigate certain aspects of cyber conflict systematically. Here, we focus on the relationship between cyber-operations (COs)[1] and conventional disputes[2] as a tractable, useful, and consequential point of departure for a fuller understanding of this important topic. *What determines when states use COs along side, or alternately instead of, traditional tools of conflict? Could the relationship between cyber and conventional conflict prove complex or indirect?* Current thinking on the relationship between cyber and conventional conflict is somewhat dialectical. Cyber "revolutionists" characterize COs as "weapons of tomorrow" that will play a decisive role in future military conflicts (Clarke and Knake 2010; Kello 2013). Since COs can exploit vulnerabilities about which a target may initially be unaware, they offer the potential to quickly disrupt an opponent's command and control, hinder communications, or otherwise obstruct government activities and military operations. As COs rise in prominence and performance, it is even possible that warfare in cyberspace will supplant traditional forms of conflict.[3]

Yet, there are reasons to question such causal claims, or at least qualify their empirical scope or significance. Cyber "evolutionists" argue in contrast that conflict in cyberspace is not likely to supplant other forms of conflict. Since cyber disruptions tend to be temporary and limited, they may only prove adequate to coerce targets in relatively minor contests (Gartzke 2013; Rid 2012; Valeriano, Jensen, and Maness 2018). Because of this, and because conventional capabilities are often required to secure cyber gains, evolutionists argue that COs are better thought of as complements to traditional modes of combat, rather than as substitutes.

The current debate thus focuses on different interpretations of the *direct* relationship between cyber conflict and other domains of disputation. But existing theories fail to consider the possibility of an *indirect* relationship between cyber and conventional conflict. Previous studies also fail to provide systematic evidence to support (or refute) any claims linking virtual and terrestrial conflict behavior. We introduce a variable—a country's Internet access—that *indirectly* links both forms of conflict. We argue that with an increase in a country's Internet access, it is more likely to initiate or become a target of cyber conflict, but that it is also less likely to initiate or become a target of conventional conflict. The Internet not only makes virtual warfare possible, but it also shapes the issues over which states and citizens compete (e.g., rising value of information).

To test our theory, we introduce a novel estimation approach to evaluate complementarity and substitutability in different forms of conflict behavior. This approach allows us to differentiate between concurrent and sequential[4] use of cyber and conventional military operations, making it possible to establish whether and how virtual and conventional conflict each impact the other. We apply our estimation approach to two datasets: the Dyadic Cyber Incident Dataset (Valeriano, Jensen, and Maness 2018) and the Militarized Interstate Disputes (MIDs) dataset (Maoz 2005).

In addition to robust empirical support for our theory, our findings also reveal the effect of additional variables on a country's decision to engage in cyber or conventional conflict. Specifically, the fact that a target possesses (shares) nuclear weapons increases the likelihood of a state using less escalatory means to resolve a dispute—cyber operations or MIDs. Geographical distance between states appears irrelevant for both types of conflict. Given the rapid spread of the Internet in recent decades, it is not surprising that the distance between two states does not significantly affect the ability of rivals to engage in digital or physical exchanges.[5] Lastly, we show that national capabilities differentially shape the propensity to engage in cyber and conventional conflict.

This study makes several contributions. First, our findings shed light on the behavior of rivals in digital and conventional domains. Similarly to Valeriano and Maness (2014), we show that rivals use every tool at their disposal to hurt one another, but unlike the authors we provide systematic empirical evidence that rivals tend to use cyber and conventional operations independently in pursuit of this overarching goal. Second, previous studies focus on the direct link between the two modes of conflict; we instead introduce a mechanism—a country's Internet access—that shapes both fronts, indirectly causing the substitutability between them. This evidence suggests a modest basis for the claims of Cyber Revolutionists. Finally, our findings affect the broader literature on the effect of technology on the balance of power and countries' ability to fight, even as they speak to the shape, nature, and conduct of future conflict patterns within, and across, the digital domain.

Military Technologies as Substitutes or Complements

There is a wealth of literature in the study of international security that examines military technologies as substitutes or complements. Most of the existing works on how actors confront one another (i.e. the choice of method) focus on non-cyber technologies in making this type of argument. For example, examining the complementarity between nuclear and conventional capabilities, Monteiro and Debs (2014) and Paul (2012) show that conventionally weak states are likely to seek nuclear weapons as an "equalizer." Horowitz and Narang (2014, 509) show that nuclear, chemical, and biological weapons function as complements at the pursuit stage, but once a country has acquired nuclear weapons, it is less likely to pursue other types of weapons of mass destruction, and in a few cases countries are willing to give them up, or bargain them away (Mehta 2020). Recently, scholars started paying attention to cyber technologies as substitutes or complements. Investigating China's decision to substitute space, cyber, and conventional missile weapons for nuclear weapons, Cunningham (2022) argues that the country uses this substitution as a source of strategic leverage in limited wars because it cannot respond to a worsening threat environment and credible threats with nuclear weapons or large conventional forces.

As explained earlier, the existing scholarship on cyber and conventional technologies focuses on the direct link between the two. In the sections below, we start with

summarizing the main arguments of the advocates of this direct link—cyber operations as complements or substitutes of conventional operations. Next, we introduce a missing link in existing explanations and show how a country's Internet access helps account for a government's increasing propensity to utilize COs, as opposed to conventional military operations.

A Direct Link: Cyber operations used in addition to or instead of military operations

Here we summarize existing scholarship on the two tendencies that describe the direct relationship between cyber and military operations: countries can use them as either complements or substitutes to one another. When formulating our hypotheses, we pursue the main goal of this study: to conduct systematic empirical analysis of these two claims, deriving aggregate relationships (i.e., average treatment effects) between cyber and military operations.

Complementarity

Scholars agree that COs have a limited ability to coerce.[6] Instead, governments have been using COs to affect the balance of military power during combat operations. COs can exploit a target's unrecognized vulnerabilities, offering commanders the ability to quickly disrupt an opponent's command and control, hinder communication, and create other obstacles to sustaining military operations. In the Ukrainian conflict in Donbass, for example, hackers inundated the communications of combat units and commanders by flooding their phones with text messages and phone calls, collected operational intelligence via hacked closed-circuit television cameras, intercepted drones, and obtained control of Wi-Fi access points (Kostyuk and Zhukov 2019). Yet, attacking countries must still use conventional capabilities to secure tangible gains, further suggesting that COs complement, rather than substitute for, conventional combat operations (Liff 2012). Thus, once a conventional dispute is ongoing, COs may be utilized to complement physical denial strategies on the ground.

While some COs are important during combat, others are most valuable prior to conflict onset. Cyber espionage, which can prove fruitful on an ongoing basis, is especially useful in the lead-up to an active contest. For example, many of the cyber espionage campaigns associated with the Ukrainian conflict were initiated years prior to the onset of hostilities.[7] While some espionage operations continued during the conflict (e.g., Armageddon), many stopped—some due to their diminishing informational value, while others had become compromised (Kostyuk and Zhukov 2019).

The above discussion highlights two distinct temporal dimensions of complementarity: co-occurrence and sequentiality. Co-occurrence involves operations in different domains happening more-or-less simultaneously. For instance, the fighting factions in the Ukrainian conflict used disruption operations during conventional combat. Sequentiality occurs when operations in one domain shape conflict in another

domain, at a later time. For example, the intelligence obtained by cyber-espionage preceding military operations in Ukraine was used in later combat. When formulating our hypotheses, we consider both forms of complementarity. Specifically, *Hypotheses 1A* and *1B* summarize existing scholarly perspectives on complementarity of cyber and military operations.

- *Hypothesis 1A: Co-occurrent Complementarity*—There is positive correlation between cyber operations in period t and military operations in period t.
- *Hypothesis 1B: Sequential Complementarity*—There is positive correlation between cyber operations in period $t - 1$ and military operations in period t.

Substitution

Rather than attempting to initiate costly conventional conflicts, states can use COs to degrade or destroy enemy capabilities in peacetime. These operations allow leaders to deny responsibility for damaging, invasive, or compromising operations and, as a result, they lower the chance of retaliation from the target, as well as limiting blowback at home, compared with traditional tools. Consequently, states that lack the motivation to act in another, costlier domain may deem cyber an attractive alternative.

States can potentially use COs meant to sabotage a target's networks, operations, or systems instead of conventional military operations (Borghard and Lonergan 2017; Valeriano, Jensen, and Maness 2018). The Stuxnet worm, allegedly designed by the United States and Israel, was intended to slow the development of the Iranian nuclear enrichment program, is an example of such operations. Stuxnet was a part of Operation Olympic Games—a covert, unacknowledged sabotage campaign by the United States and Israel that targeted Iranian nuclear facilities using cyber means. Olympic Games came into existence as U.S. officials sought an alternative to military operations to delay progress of Iran's nuclear enrichment program. The George W. Bush administration initiated Olympic Games in 2006, believing that the operation would prevent Israel from launching air strikes on Iranian nuclear facilities, an act that might have involved the United States in yet another major conflict in the Middle East (Sanger 2012).

As explained earlier, we consider both co-occurent and sequential manifestations of substitution when formulating our hypotheses. *Hypotheses 2A* and *2B* summarize existing scholarly perspectives on substitution of cyber and military operations.

- *Hypothesis 2A: Co-occurent Substitution*—There is negative correlation between cyber operations in period t and military operations in period t.
- *Hypothesis 2B: Sequential Substitution*—There is negative correlation between cyber operations in period $t - 1$ and military operations in period t.

The Indirect Link

In the previous paired sections, we summarized existing views that directly link cyber and conventional operations, as either complements or substitutes for one another. Below, we introduce our own argument of indirect substitution between the digital and kinetic fronts. We start by providing reasons that these two types of domains are likely to operate independently of each other, at least initially. We then introduce the missing link—Internet access—that connects the two modes of fighting, indirectly triggering substitution between them. Specifically, we argue that a country's increasing Internet access is likely to be associated with more cyber conflict and less conventional conflict.

Independence

While it is certainly plausible that COs interact with conventional conflict, it is also possible for conflict in one domain to function independently of conflict in other domains. At minimum, this prospect should be considered for logical completeness; nothing appears to obviously preclude cyber and terrestrial conflict from being occasionally, often, or even generally uncoordinated. Independence might diminish over time or vary cross-sectionally (nationally or dyadically), but complements or substitutes may be limited in an initial phase of the emergence of cyber conflict, as governments deploy capabilities that are as yet poorly integrated with other defense capabilities.

It is actually quite difficult to coordinate complex activities in different domains. Amphibious warfare has famously been considered the most difficult kind of warfare in the 20th century, precisely because it *requires* the careful orchestration of operations on land, sea, and air. Given the nature of social activities, and the all-too-human tendency to "keep things simple," unless there is a compelling reason to make such a coordinated effort — or conversely, a strong case has been made to commanders *not* to operate independently in one or several domains — the tendency would presumably be for actions taken in different domains to tend to occur independently of one another.

There is some evidence already of a lack of coordination between cyber and terrestrial domains. Using daily accounts of disruptive cyber attacks and military operations from the Syrian and Ukrainian conflicts, Kostyuk and Zhukov (2019, 319) find that while there is a tit-for-tat response for military operations, COs seem to operate in their own "bubble." The authors explain this result in terms of force synchronization: "the lead time required to plan and implement a successful attack—studying the target system, collecting intelligence on its vulnerabilities, and writing code that exploits them—can make these efforts difficult to synchronize with conventional operations" (Kostyuk and Zhukov 2019, 322).

Another reason for the possible lack of coordination between conventional conflict and cyberspace is that the logic and objectives of contests differ across different domains (Gartzke and Lindsay 2019). If cyberspace and physical space do different things, it is perhaps not that surprising that they are engaged differently, at different

times, and in different ways. As an informational domain, cyberspace is primarily useful for conveying and containing, facts. Data is easy to move through the Internet; that is what the cyber domain does. Indeed, a key problem in cyberspace is limiting the diffusion of information. Organizations, including governments, seek to limit who knows what, when, and where. This implies that critical objectives in cyber conflict involve the control of information, as opposed to territory, tangible goods (such as airports or equipment) or institutions (like government offices or a leader).

Based on these perspectives, we argue that states are likely to use conventional military operations and COs largely independently, at least for now. Thus, we are unlikely to find significant complementarity or substitution across cyber and military operations.

- *Hypothesis 3A: Co-occurent Independence*—Cyber operations in period t and military operations in period t operate independently of each other.
- *Hypothesis 3B: Sequential Independence*—Cyber operations in period $t-1$ and military operations in period t operate independently of each other.

Internet Access and Modes of Conflict

If cyber conflict does not interact with conventional conflict directly, is there a mechanism that could potentially connect the two indirectly, given at least the coincidental rise in cyber conflicts (Karatzogianni 2015) and a corresponding decrease in conventional conflicts (Holsti 2016)? Previous research suggests a number of mechanisms capable of explaining the decline in interstate conflicts since 1945, including norms development, changing power distributions, and the spread of knowledge of how to avoid the use of armed force (Holsti 2016). In the section on substitution, we explained the benefits of using cyber operations over conventional operations, leading to a potential rise of the former. But there are no studies that explicitly consider a mechanism that could link the two phenomena, simultaneously explaining changes in both cyber and conventional fronts.

The spread of the Internet is one such mechanism, as the advent of cyberspace affects both virtual and terrestrial modes of fighting, indirectly causing substitution between them.[8] Two conditions must be met for this indirect relationship to hold. First, cyberspace as a domain must facilitate "useful" forms of international conflict. Second, traditional domains for conflict must no longer be adequate or functional to achieve competitors' aims. We discuss each necessary condition in turn.

Cyberspace facilitates "useful" forms of international conflict. Internet or cyberspace is an artificial domain, created entirely by human artifice. The processes that led to cyberspace are at least trivially responsible for COs, as clearly there can be no cyber conflict without cyberspace. But, the mere presence of a venue for conflict does not mean that (much) conflict will occur if actors have no reason to disagree in a specific manner, or if the domain does not lend itself to both prosecuting and practical resolution of differences. Space, for example, was initially thought to be an important emerging

domain for political violence. Yet, it quickly became clear that this ultimate "high ground" was much more useful as an observation post than as a firing platform. Space was hard to get to and difficult to operate or maintain equipment and weapons in, while occupation was problematic and "control" offered only limited types of advantages to a competitor.

Like space, cyberspace can be considered more an observation post than a weapons platform, but this distinction quickly becomes blurred due to ambiguities about the nature of cyber "weapons." In space, observation is free and open, provided one can get there. Surveillance satellites peer down on earth with only limited natural or artificial obstruction. Because spying from space cannot be prevented, there is no need for nations to keep their espionage efforts secret. Since everyone knows about "eyes in the sky," the effect of space surveillance is disproportionately deterrence. Nations are discouraged from actions that would be degraded by revelation because they cannot conceal them.[9]

Cyber espionage, in contrast, is preventable (at least potentially). Because of this, spying must be pursued in secret, even as penetrating other actors' networks involves actions and measures that look much more like warfare than does deploying cameras in the sky. Revelation of cyber-espionage activities typically degrades future access to sources of information. The secrecy that must be maintained to operate clandestinely in cyberspace means that COs are more like traditional espionage than space surveillance. Indeed, the penetration of enemy systems required for cyber-spying may be indistinguishable to targets from efforts designed to degrade or destroy these same systems. Access is essential and contested, whether one is preparing an attack or just listening.

Information has been a valuable currency and a concern in warfare for centuries (Fearon 1995). But information has become an even more attractive commodity in the information age. Knowledge has been an ascendant component of wealth and power for millennia, but it has arguably never been more important than it is today. While there are multiple ways to access insights about the world (e.g., human and signals intelligence sources), cyberspace is an attractive environment in which to manage, distribute, and obtain information.

The world's governments are increasingly turning to the Internet or cellular technology to obtain secrets or access compromising information about foreign governments or important individuals. China, notably, has made extensive use of COs to acquire military and civilian industrial technology from the West. Western nations have also increasingly relied on cyberspace as a domain of espionage. For example, the US National Security Agency (NSA) partnered with Danish intelligence officials to monitor the Internet traffic of European leaders (Henley 2021). While German leaders like Angela Merkel expressed outrage, Germany has its own tradition of spying on friends and neighbors (Dobson 2020). There are of course many other examples, only some of which are known to the general public, given the covert nature of a high proportion of COs.

As these examples suggest, cyberspace is an extremely attractive domain for both aggressors and targets, given their respective objectives. Chinese spies could, and have,

sought to obtain sensitive technologies through physical means, but these operations are costly, risky, and difficult to conceal. The theft of intellectual property through cyberspace can be conducted by operators that are physically remote from a given target. At the same time, targets continue to house sensitive data in the virtual domain, due to the benefits of managing and disseminating information in cyberspace.

The examples above suggest the nature or contexts where COs are more attractive as a mode of conflict. Governments appear to prefer acting in cyberspace when their costs are low and their objectives are readily obtainable. Obviously, this is not always the case. The increasing value and availability of knowledge and information make COs more useful tools for states that also have economies that are, or seek to be, structured around informational technologies. A high level of Internet access both reflects and effects the value of information in a nation's economy, even as using conventional tools of conflict to obtain information is much less effective.

The second necessary condition is that traditional domains for conflict must no longer be adequate or functional to achieve competitors' aims. For much of history, the foundations of civilization rested on control and exploitation of physical territory. More land meant more wealth. Today, prosperity is no longer derived primarily from agriculture, or from extracting minerals from the soil. Much more of the productive (and destructive) capacity of states rests with human and financial capital. Unlike empires of the past, modern nations seldom seek conquest and plunder to sustain and enrich themselves.[10] Instead, they use or threaten force to extract political concessions—to tell others how they must behave, not what property they can possess—rather than taking territory or other tangible goods.

This transition in the motives of states has begun to transform international conflict. Long the focus of military aggression, territorial conquest holds less appeal it once did (Gartzke and Rohner 2011). Modern armies largely refrain from the venerable tactics of raid and pillage, not due to superior morals, but because there is little profit in using extremely expensive organizations to steal relatively cheap stuff. With the decline in the value of territory as a means of achieving wealth and power, the utility of conventional conflict has also declined, at least in its most traditional forms. Military violence remains, but it is much more focused on the projection of influence or the acquisition of strategic territory, than on physical conquest. Force is used to punish, coerce or deny, not to take.[11]

The global spread of the Internet increased the need to acquire and control information. Cyberspace is a great medium of ideas, those that owners wish to share as well as those they do not. If information is power, then increasingly contestation is over the control of information, raising the value of the stakes over information as a commodity. While COs are not limited to espionage, the need to gain access, regardless of one's motives for doing so, and the range of actions that are possible, once access has been achieved, mean that a high proportion of COs will look like espionage. Indeed, most COs contain elements of spying, regardless of what other objectives may be planned or contemplated. Put more simply, spying is where conflict is at in cyberspace.

By the same token, it is not always clear that conventional military force is likely to advantage actors seeking to acquire or control information. Airstrikes, fishing disputes or border clashes seldom penetrate or compromise a target's command-and-control apparatus, the industrial secrets of leading firms, or a party headquarters. Similarly, while airstrikes can damage an opponent's capabilities such as, for example, nuclear enrichment facilities, they are not subtle. Kinetic attacks often cause collateral or environmental damage and leave an attacker open to international condemnation and possible retribution. In contrast, COs can allow an attacker to rebalance power anonymously, further demonstrating why using COs is cheaper than conventional tools.

COs possess several drawbacks in pursuing the traditional goals of military force. These drawbacks include problems like limited destructiveness, a minimum of psychological shock, the temporal boundedness of damage, and a lack of credibility. At the same time, their strengths play to exactly the needs of a growing list of nations in the 21st century, while also offering a contrasting set of advantages from conventional modes of conflict. COs allow actors to benefit at a target's expense (shifting the balance of power) at relatively low cost and risk of escalation. They are particularly practical when the stakes in a contest involve intangibles (information, control, and actors' beliefs).

Thus, cyberspace is unlikely to yield an indirect complementarity between different domains of conflict. If a country can use cyber to obtain sensitive information to shift the balance of power, it has few incentives to also execute a more costly military action.[12] Instead, we expect cyberspace to produce an indirect substitution between different conflict domains. Given the growing value of information, nations are mostly interested in using cyberspace to achieve these new objectives. But not all nations can. Increasing a country's Internet access is likely to lead to an increase in that country's propensity to engage in cyber conflict, and to reduce the nation's likelihood of engaging in conventional conflict. *Hypotheses 4A* and *4B* summarize these views below.[13]

- *Hypothesis 4A: Attacker's Internet Access & Indirect Substitution*—With an increase in a country's Internet access, it is likely to participate in *more cyber* conflicts and in *fewer conventional* conflicts.
- *Hypothesis 4B: Target's Internet Access & Indirect Substitution*—With an increase in a country's Internet access, it is likely to become a target of *more cyber* conflicts and of *fewer conventional* conflicts.

Since the critical objectives in cyber conflict involve the control of information, the "main event" in cyber conflict is espionage, as well as valence activities designed to facilitate or interrupt spying. Other things happen in cyber conflict, such as denial of service attacks and attempts to undermine or obstruct control systems (e.g. Stuxnet), but a large portion of cyber activities are related to the control of information, rather than places or things.[14] This point aligns with the recent scholarship which views actors' behavior in cyberspace primarily as an "intelligence contest" (Chesney et al. 2020).

If the Internet is largely a place for stealing information from others or alternately protecting one's own information, then we are more likely to observe the indirect substitution of cyber espionage operations with conventional operations than such substitution of disruption and degradation operations with conventional operations. This is because the main goal of cyber espionage is to "steal critical information or manipulate information asymmetries in a manner that produces bargaining benefits between rival states engaged in long-term competition," whereas disruption and degradation COs that target networks or systems are less useful in obtaining information (Valeriano, Jensen, and Maness 2018, 11-12). As a result, we hypothesize that increasing a country's Internet access is likely to lead to an increase in that country's propensity to engage in, and defend against, cyber espionage, and to reduce (somewhat) a nation's utility for engaging in conventional operations. *Hypotheses 5A* and *5B* summarize these views below.[15]

- *Hypothesis 5A: Attacker's Internet Access, Cyber Espionage & Indirect Substitution*—With an increase in a country's Internet access, it is likely to participate in *more cyber*-espionage operations and in *fewer conventional* operations.
- *Hypothesis 5B: Target's Internet Access, Cyber Espionage & Indirect Substitution*—With an increase in a country's Internet access, it is likely to become a target of *more cyber*-espionage operations and of *fewer conventional* operations.

Data

This section explains key details of the datasets we use to conduct our analysis. We start this section by explaining the choice of our population, interstate rivalries. We then briefly describe the datasets on COs taken from Valeriano, Jensen, and Maness (2018)'s Dyadic Cyber Incident Dataset (v1.5) and on conventional operations taken from Maoz (2005)'s Militarized Interstate Disputes data. By combining both DCID and MIDs datasets, we are able to study conventional military campaigns that may or may not involve the use of COs and cyber campaigns that may or may not involve conventional operations. Together, these data contain 2,300 dyad-year observations.[16] We end with an explanation of how we measure a set of controls that help us further assess the empirical validity of our hypotheses on interdependencies between cyber and conventional conflict.

Identifying the Population of Rivalries

This study seeks to determine why nations choose particular domains in which to fight. Rivalries are ideal for this purpose, since they involve pairs of nations with demonstrated hostility, but that may or may not fight in a given time period. Samples of rivalries generally capture around 80 percent of interstate conflict over the past two hundred years (Thompson and Dreyer 2011). To identify conventional rivalries, we use Thompson and Dreyer (2011)'s "diplomatic history" approach, according to which

states are rivalries if they view one another as "(a) competitors, (b) the source of actual or latent threats that pose some possibility of becoming militarized, and (c) enemies" (Thompson 2001, 560). Since we are interested in explaining when states use cyber, conventional, or both types of operations, we combine the dyads identified as conventional rivalries in Thompson and Dreyer (2011) with the dyads identified as cyber rivals in Valeriano and Maness (2014) to create the population of rivalries that we use in our analysis.

A focus on rivalries also allows us to favorably assess the complement/substitution arguments (*Hypotheses 1* and *2*), while likely biasing against our theory (*Hypotheses 3— 5*). Nations that experience few conventional disputes do not qualify as rivals. As such, the predictions of our indirect argument, if fulfilled, will lead more states with a high Internet access and dyads to be under-counted as conventional rivals, compared to states that have a low Internet access; though, states with a high Internet access may continue to exhibit a significant number of cyber conflicts than states with a low Internet access. More generally, it is difficult to assess how countries might behave differently in terms of their conflict behavior if they exhibit little or no conflict. Another reason why we focus on rivalries is a practical limitation that we face—the dataset of COs that we utilize relies on rivalries for its sampling approach (Valeriano and Maness 2014).

Cyber Conflict Data

Valeriano, Jensen, and Maness (2018)'s Dyadic Cyber Incident Dataset (DCID) (v1.5) defines a cyberincident as an accumulation of individual COs to achieve a strategically important goal. For example, these data code cyberattacks against Estonia that lasted for about 3 weeks in 2007 as one incident. `Cyber` takes the value of 1 when an attacker initiated a cyberincident against a target and 0 when the attacker did not initiate a cyberincident against the target during the period under study.

We use DCID for the following reasons. First, a cyberattack rarely occurs in isolation; generally a series of attacks occur together. Second, by focusing on incidents instead of individual attacks, we can assess the importance of the overall cyber effort to larger national objectives. Third, DCID is one of (only) two available data sources of COs.[17] Fourth, we follow existing political science scholarship that uses DCID to examine the dynamics of non-cyber international trends (i.e., interstate trade in Akoto (2021)).

Variations in reporting can be a serious problem for conflict event data (Weidmann 2016), especially for COs, due to their novelty, secrecy surrounding their execution and the difficulty of attributing origin. These factors might be valid concerns even though DCID follows a well-established practice in conflict studies by using multiple sources to record an event (Gohdes and Carey 2017). Yet, bias may not present as serious an issue here as one might assume. While individual attacks might be unreported or undiscovered, it is much more difficult not to notice a full-scale cyberincident.[18] At the same time, it much easier to use multiple sources to mistakenly record an individual cyberattack, which often lacks specific details, than to over-report large-scale

cyberincidents. Misattribution or inattention is thus least likely in the context of the rivalry sample used by the DCID data, given that private cyber security firms seek to unearth and publicize large-scale COs since doing so brings them publicity, new clients, and increased revenue.[19]

Military Conflict Data

We use the presence of a militarized interstate dispute (MID) between two states to measure conventional military conflict (Maoz 2005). Gochman and Maoz (1984, 587) define MIDs as "a set of interactions between or among states involving threats to use military force, displays of military force, or actual uses of military force." `Military` is coded 1 when an attacker initiated an MID against a target and 0 otherwise.[20] The MIDs data is the most suitable data (yet available) to study the subject of our inquiry for the following reasons. First, since we are interested in understanding how cyber is being used along conventional military operations, it makes sense to look at the cases that include "display…of military force" recorded in the MIDs data (Jones, Bremer, and Singer 1996, 163). Second, COs are often viewed as instances "short of war" (e.g., Liebetrau 2022). The MIDs data includes such instances as well (i.e., "use of military force short of war") (Jones, Bremer, and Singer 1996, 163).[21]

Independent Variables

We consider a number of variables that might affect a nation's willingness to fight. Our key independent variable is *Internet access*, measured by Internet users per capita,[22] taken from the World Bank.[23]

To address the possibility that substituting cyber-capabilities may be more attractive than other types of conflict for weak (or unresolved) actors, relative to their opponents, we account for the level of *national capabilities* taken from Singer, Bremer, and Stuckey (1972)'s Composite Index of National Capability score (v5.0). To address the possibility that states that share borders are more likely to use conventional weapons whereas those that are further away resort to cyber means, we control for the *distance* between states, using the inverse distance between their capitals. Lastly, the stability-instability paradox argues that nuclear weapons deter high-intensity contests but encourage lower-intensity disputes (George and Smoke 1974). States might similarly substitute COs for conventional operations as the former are less disruptive. We therefore control for whether a target possesses or shares nuclear weapons.[24]

Empirical Strategy

Complementarity versus Substitutability

While notions of complementarity and substitutability are widely applied in political science, differences exist in how these two concepts relate temporally. Assuming a

sequential interpretation prioritizes the dynamic development of paired phenomena. Applying this definition in our context, complementarity is a positive correlation between cyber operations in period $t - 1$ and military operations in period t; and substitutability is a negative correlation between cyber operations at $t - 1$ and military operations at t.

The second assumption one can make about ties is the co-occurrence of paired phenomena. Using this interpretation, complementarity is a positive correlation between cyber operations in period t and military operations in period t; and substitutability is a similar negative correlation. Studying such co-occurrences empirically is difficult, however. If we condition on the variable from the same time period, we risk conditioning on the future since we do not know the ordering of events; this could lead to reverse causality and biased estimates of the model parameters.

To determine whether digital and conventional conflict domains shape each other sequentially or concurrently (or not), we introduce a new approach that estimates both versions of complementarity and substitutability. A logistic regression with lagged dependent variables approximates sequential effects of cyber and conventional conflict. We allow for concurrent substitution or complementarity by jointly estimating factors associated with cyber and conventional operations while using a random slope for operation "type" to model dependence among conflict outcomes in a given dyad and time period. Joint estimation also constrains associations between covariates with cyber and conventional outcomes to be equal (or not) through interactions with operation type. Online Appendix Section 2 provides a detailed explanation of our empirical strategy that accounts for both concurrent substitution and complementarity of cyber and military operations.

Findings

Results

Tables 1 and 2 present our results. Table 1 includes a number of models, starting with the base model with no covariates to the model that accounts for the effect of each covariate on the likelihood of different types of conflict—cyber, conventional, or any (cyber and conventional). Table 2 displays the results for different types of cyber-operations. Our main findings are that a rival's Internet access explains its propensity towards cyber versus conventional conflict. This is especially the case for cyber-espionage operations.

We start with testing our primary hypotheses of indirect substitution (*Hypotheses 4A* and *4B*) and find support for them. Specifically, with an increase in its Internet access, a state is more likely to use cyber means, and less likely to use conventional means, to engage in conflict (*Hypothesis 4A*). The expected odds[25] of a cyber conflict are 1.78 (Model 4 in Table 1)–2.15 (Model 1 in Table 1) times greater and the expected odds of a conventional conflict are 0.68 (Model 2 in Table 1)–0.78 (Models 4 & 5 in Table 1) times lower for each unit standard deviation increase of the attacker's (log) Internet

Table 1. The Likelihood of Using Cyber and Conventional, Military Operations, by Rivalries (Odd Ratios and Confidence Intervals).

	Model 1	Model 2	Model 3	Model 4	Model 5
			Fixed effects		
			Dependent Variable: Probability of cyber conflict in period t		
Cyber conflict in period t-1	28.99***(13.68; 61.44)	15.30***(7.09; 33.03)	14.53***(6.62; 31.88)	14.58***(6.64; 32.02)	14.57***(6.63; 32.01)
Conventional conflict in period t-1	0.57(0.26, 1.25)	0.69(0.31; 1.54)	0.55(0.24; 1.23)	0.54(0.24; 1.23)	0.54(0.24; 1.22)
Attacker's internet users per capita (log, sc)	—	2.15**(1.33; 3.46)	1.79*(1.12; 2.87)	1.78*(1.11; 2.86)	1.79*(1.11; 2.86)
Target's internet users per capita (log, sc)	—	2.00**(1.23; 3.24)	2.26**(1.37; 3.72)	2.27**(1.37; 3.75)	2.27**(1.37; 3.75)
Attacker's CINC score (sc)	—	—	2.77***(1.88; 4.09)	2.83***(1.88; 4.25)	2.83***(1.88; 4.25)
Distance between two states (sc)	—	—	—	1.12(0.71; 1.79)	1.13(0.71; 1.80)
Nuclear-armed target (dummy)	—	—	—	—	2.81*(1.07; 7.41)
			Dependent Variable: Probability of conventional conflict in period t		
Cyber conflict in period t-1	1.01(0.48, 2.13)	1.25(0.58; 2.67)	1.42(0.67; 3.02)	1.42(0.67; 3.02)	1.41(0.66; 3.01)
Conventional conflict in period t-1	5.96***(3.92, 9.07)	5.62***(3.70; 8.52)	5.79***(3.82; 8.79)	5.79***(3.82; 8.79)	5.80***(3.82; 8.80)
Attacker's internet users per capita (log, sc)	—	0.68*(0.50; 0.93)	0.77(0.57; 1.05)	0.78(0.57; 1.05)	0.78(0.57; 1.05)
Target's internet users per capita (log, sc)	—	0.73*(0.54; 0.98)	0.71*(0.53; 0.96)	0.71*(0.53; 0.96)	0.72*(0.53; 0.97)

(continued)

Table 1. (continued)

	Model 1	Model 2	Model 3	Model 4	Model 5
Attacker's CINC score (sc)	—	—	1.10(0.79; 1.53)	1.09(0.78; 1.53)	1.10(0.78; 1.53)
Distance between two states (sc)	—	—	—	1.04(0.72; 1.49)	1.04(0.72; 1.49)
Nuclear-armed target (dummy)	—	—	—	—	2.62*(1.20; 5.71)
Dependent Variable: Probability of any conflict in period t					
Attacker's internet uses per capita (log, sc)	0.91(0.70, 1.18)	1.21(0.89; 1.63)	1.18(0.87; 1.60)	1.18(0.87; 1.60)	1.18(0.87; 1.60)
Target's internet uses per capita (log, sc)	0.93(0.72, 1.19)	1.20(0.89; 1.62)	1.27(0.93; 1.73)	1.27(0.93; 1.74)	1.27(0.93; 1.74)
Attacker's CINC score (sc)	1.65***(1.26, 2.16)	1.67***(1.25; 2.22)	1.75***(1.30; 2.36)	1.76***(1.30; 2.38)	1.76***(1.30; 2.38)
Distance between two states (sc)	1.04(0.77, 1.40)	1.05(0.77; 1.44)	1.07(0.77; 1.47)	1.08(0.78; 1.51)	1.08(0.78; 1.51)
Nuclear-armed target (dummy)	2.19*(1.15, 4.15)	2.47**(1.25; 4.88)	2.67**(1.32; 5.39)	2.68**(1.33; 5.42)	2.71**(1.32; 5.59)
Random Effects					
Dyad (intercept)	✓	✓	✓	✓	✓
Variance	1.02	1.22	1.36	1.36	1.36
Dyad (slope for `Type`)	✓	✓	✓	✓	✓
Variance	0.30	0.61	0.31	0.31	0.30
Akaike Inf. Crit.	1389.2	1348.6	1328.5	1330.5	1332.4

Note: Results are from a logistic regression model. The reported values are the odds ratios and confidence intervals. Odds ratio larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,300 observations. All results are based on two-tailed tests. Variables: `log`—logarithmized; `sc`—standardized. ^$p < 0.1$; *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

Table 2. The Likelihood of Using Cyber and Conventional, Military Operations, by Rivalries and Types of Cyber Operations (Odd Ratios and Confidence Intervals).

	Model 6	Model 7	Model 8	Model 9
	Espionage w/o controls	Espionage w/ controls	Disruption & Degradation w/o controls	Disruption & Degradation w/ controls
Fixed effects				
Dependent Variable: Probability of cyber conflict in period t				
Cyber conflict in period t-1◊	220.5***(57.0, 852.1)	187.1***(45.1, 776.1)	3.91*(1.30, 11.72)	3.28*(1.12, 9.63)
Conventional conflict in period t-1	0.58(0.17, 2.02)	0.56(0.16, 1.90)	0.63(0.24, 1.68)	0.66(0.25, 1.72)
Attacker's internet uses per capita (log, sc)	3.21***(1.65, 6.24)	2.49**(1.25, 4.93)	1.14(0.68, 1.90)	0.89(0.51, 1.53)
Target's internet uses per capita (log, sc)	3.21***(1.65, 6.24)	2.49**(1.25, 4.93)	1.14(0.68, 1.90)	0.89(0.51, 1.53)
Attacker's CINC score (sc)	—	2.56***(1.68, 3.88)	—	1.88**(1.22, 2.88)
Dependent Variable: Probability of conventional conflict in period t				
Cyber conflict in period t-1◊	1.00(0.38, 2.65)	1.01(0.39, 2.63)	1.88(0.66, 5.38)	1.84(0.65, 5.25)
Conventional conflict in period t-1	6.06***(3.93, 9.36)	6.31***(4.10, 9.70)	5.59***(3.67, 8.52)	5.77***(3.80, 8.78)
Attacker's internet uses per capita (log, sc)	0.82(0.61, 1.09)	0.79(0.59, 1.06)	0.77(0.57, 1.05)	0.77^(0.57, 1.04)
Target's internet uses per capita (log, sc)	0.82(0.61, 1.09)	0.79(0.59, 1.06)	0.77(0.57, 1.05)	0.77^(0.57, 1.04)
Attacker's CINC score (sc)	—	1.16(0.85, 1.58)	—	1.08(0.78, 1.50)

(continued)

Table 2. (continued)

	Model 6	Model 7	Model 8	Model 9
	Espionage w/o controls	Espionage w/ controls	Disruption & Degradation w/o controls	Disruption & Degradation w/ controls
Dependent Variable: Probability of any conflict in period t				
Attacker's internet uses per capita (log, sc)	1.62*(1.11, 2.37)	1.40^(0.95, 2.07)	0.94(0.68, 1.30)	0.82(0.59, 1.15)
Target's internet uses per capita (log, sc)	1.62*(1.11, 2.37)	1.40^(0.95, 2.07)	0.94(0.68, 1.30)	0.82(0.59, 1.15)
Attacker's CINC score (sc)	—	1.72***(1.27, 2.33)	—	1.42*(1.05, 1.93)
Distance between two states (sc)	—	1.08(0.79, 1.48)	—	1.02(0.73, 1.42)
Nuclear-armed target (dummy)	—	2.12*(1.06, 4.22)	—	3.28***(1.62, 6.65)
Random Effects				
Dyad (intercept)	✓	✓	✓	✓
Variance	1.34	1.16	1.21	1.09
Dyad (slope for `Type`)	✓	✓	✓	✓
Variance	0.37	0.21	0.82	0.73
Akaike Inf. Crit.	1186.2	1165.2	—	1213.4
Number of obs-ns	2,300	2,300	2,300	2,300

Note: Results are from a logistic regression model. The reported values are the odds ratios and confidence intervals. Odds ratio larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,300 observations. All results are based on two-tailed tests. Variables: `log`—logarithmized; `sc`—standardized; ◊ identifies similar types of operations as models DVs (e.g., in the model where cyber espionage is a DV (Model 6), the independent variable is lagged cyber espionage). ^$p < 0.1$; *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

users per capita. Moreover, with an increase in its Internet access, a state is more likely to become a target of cyber conflict and less likely to become a target of conventional conflict (*Hypothesis 4B*). The expected odds of a cyber conflict are 2.00 (Model 2 in Table 1)–2.27 (Models 4 & 5 in Table 1) times greater and the expected odds of a conventional conflict are 0.71 (Models 3 & 4 in Table 1)–0.73 (Model 2 in Table 1) times lower for each unit standard deviation increase of the target's (log) Internet users per capita.

We further confirm this indirect substitution effect of a rival's Internet access on its propensity towards different modes of conflict by showing that rivals do not use cyber and conventional military operations as concurrent complements or substitutes. While rivals are likely to sequentially use cyber and conventional operations against the same targets, they use these two types of operations independently from each other. This evidence provides support for *Hypothesis 3* and refutes *Hypotheses 1* and *2*. Specifically, the expected odds of a CO are 14.53 (Model 3 in Table 1)–28.99 (Model 1 in Table 1) times greater if a CO took place in a previous period than if no CO took place in a previous period. The expected odds of a MID are 5.62 (Model 2 in Table 1)–5.96 (Model 1 in Table 1) times greater if a MID took place in a previous period than if no MID took place in a previous period.

These findings point to two interesting phenomena. First, a higher odds ratio for the target's (log) Internet users per capita than for the attacker's (log) Internet users per capita implies that the target's Internet access plays a slightly more important role. Second, a country's reliance on the Internet is slightly pacifying in conventional terms. The positive association between the country's Internet access and its probability of getting involved in cyber conflict, combined with the negative relationship between the country's Internet access and its probability of getting involved in conventional disputes suggests a modest basis for the claims of Cyber Revolutionists.

Next we test our theoretical expectations for different types of cyber-operations. To remind, we expect cyber espionage as well as combined disruption-degradation operations to operate independently from conventional operations (*Hypothesis 3*). But we expect to find a more likely indirect substitution effect for cyber-espionage operations (*Hypotheses 5A* and *5B*) than for combined disruption-degradation operations. Table 2 displays the results. We find that rivals do not use different types of COs and conventional military operations as concurrent complements or substitutions. But they are likely to sequentially use these operations against the same targets but independently from each other. This evidence supports *Hypothesis 3* and refutes *Hypotheses 1* and *2*. Importantly, we find evidence for the indirect substitution effect of cyber-espionage operations, supporting *Hypotheses 5A* and *5B* (Models 6 and 7 in Table 2).[26] But there are no real evidence of association between disruption-degradation attacks and the Internet users (Models 8 and 9 in Table 2), as suggested by our theory.

In addition to our main results explained above, we also investigate how additional covariates help explain how different features of a given dyad affect whether countries engage in cyber and/or conventional conflict, and why. Specifically, we show that there is a positive, statistically significant association between an attacker's CINC score and

its likelihood of cyber conflict: the expected odds of a cyber conflict are 2.77 (Model 3 in Table 1)–2.83 (Models 4 & 5 in Table 1) times greater for each standard deviation increase of the attacker's CINC score. But the association between attacker's CINC score and its likelihood of conventional conflict is not statistically significant. National capability measures are often statistically insignificant (De Mesquita and Lalman 1988). But it is likely, perhaps that strategic interaction plays a critical role. Because everyone knows that power matters in winning wars, the effects of power on conflict onset are largely absorbed in expectations about relative military performance, and thus manifest through bargaining and diplomacy (a subject international relations too typically ignores), rather than through more easily observable warfare (Powell 1999).

Moreover, there is no association between distance and conflict, perhaps because the Internet allows countries to wage wars far from home. But there is a positive, statistically significant relationship between a target possessing (sharing) nuclear weapons and the probability of any dispute. The expected odds of cyber conflict are 2.81 (Model 5 in Table 1) times greater and the expected odds of conventional conflict are 2.62 (Model 5 in Table 1) times greater if the target possesses (shares) nuclear weapons than if the target does not possess such weapons. This result can be explained by a widespread perception that COs are non-escalatory, and the fact that most MIDs involve disputes short of wars.

To further assess the influence of the country's Internet access on its likelihood of engaging in either form of conflict, Figure 1 presents an interaction plot that visualizes the results from Model 3 in Table 1.[27] The *x*-axis displays the logarithmized and rescaled country's Internet users per capita and the *y*-axis displays its probability of engaging in any conflict. Figure 1a, which displays the results for the attacker, shows that as the attacker's Internet users per capita increases, its likelihood of engaging in conventional disputes decreases and its likelihood of engaging in cyber conflict increases. Figure 1b, which displays the results for the target, shows that as the target's Internet users per capita increases, its likelihood of engaging in conventional disputes decreases and its likelihood of engaging in cyber conflict increases.

Robustness Checks

Variations in reporting can be a serious problem for conflict event data (Weidmann 2016), especially for COs, due to their novelty, secrecy surrounding their execution, and the difficulty of attributing origin. As explained earlier, even though bias may not present as serious of an issue for our analysis as one might assume, we run additional tests that consider the two types of biases that can result in latent events—events that happened but are not recorded in the dataset. First is non-systematic under-reporting that occurs if variables in the model are not related to the probability that a CO is reported (e.g., COs are under-reported at random or according to the model predictions), conditional on the cyber conflict occurring. Second is systematic under- or over-reporting that occurs if variables in the model are related to the probability that a COs is reported (e.g., due to COs's transparent nature, democracies tend to report more COs

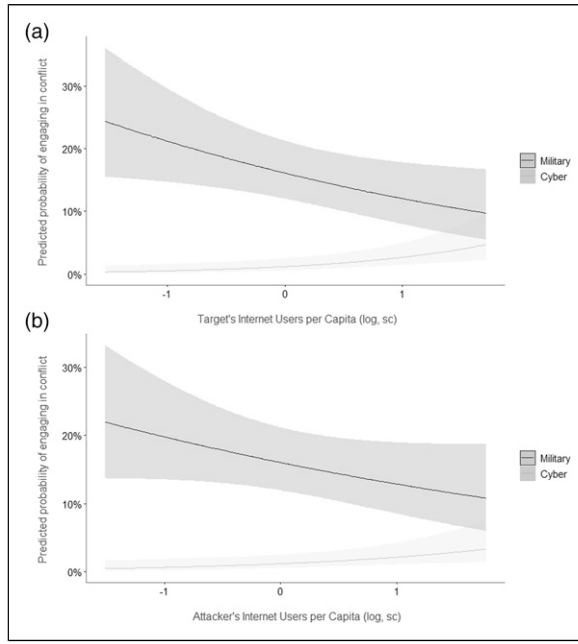

Figure 1. *Interaction Plot: Country's Internet Access and its Likelihood of Experiencing Conflict* (a) Attacker's Internet Access and its Likelihood of Experiencing Conflict (b) Target's Internet Access and its Likelihood of Experiencing Conflict. *Note:* This figure visualizes the results from Model 3 in Table 1. *x-axis:* 0 is the mean of a country's Internet users per capita; other numbers represent standard deviations from the mean. Data sources: DCID (Valeriano, Jensen, and Maness 2018) and MID data (Maoz 2005). Figure 1a shows that as the attacker's Internet users per capita increases, its likelihood of engaging in conventional disputes decreases and its likelihood of engaging in cyber conflict increases. Figure 1b shows that as the target's Internet users per capita increases, its likelihood of engaging in conventional disputes decreases and its likelihood of engaging in cyber conflict increases.

that they suffered than autocracies). The obtained results presented in Online Appendix Section 4.1 confirm that our main finding—indirect substitutability of a country's Internet dependency and its likelihood of experiencing cyber and conventional conflict—is robust to the situations that account for different types of reporting biases typical for COs.

Moreover, our findings are also robust to (an) alternative (1) model specification—instead of dyad REs, we also use dyad-year REs; (2) time dimension—instead of the yearly data we use monthly data;[28] (3) measures of covariates; (4) behavior, investigating whether cyber can be a tool used mostly by major powers; and (5) measure of lags. Online Appendix Sections 4.2-4.6 present a detailed explanation of all these results.

Discussion and Implications

Much remains to be done in assessing the impact of new forms of conflict on war and peace. We began with a pair of contrasting conventional wisdoms about how cyber and conventional conflict interact. We have provided tentative evidence that largely contradicts both of these dialectical accounts: cyber neither triggers or substitutes for conventional conflict behavior. Instead, cyber conflict exists at present largely independently from conventional military operations. Further, the decline in militarized conflict identified in recent decades cannot be explained simply by the rise of "cyberwar." To the contrary, we provide evidence for a common root in terms of technology.

Specifically, we introduced a missing link—Internet access—to explain both the decline in conventional conflict and the increase in cyber conflict. Countries have been utilizing cyberspace to pursue and control information, an increasingly attractive commodity. Given that cyberspace allows actors to compete over information, we can expect increased friction in this new medium as technologically sophisticated states pursue their strategic goals.

In addition to Internet access, our findings shed light on other factors affecting a nation's propensity to engage in cyber and/or conventional conflict. States possessing nuclear weapons are more likely to engage in any conflict, implying stability-instability, as nuclear status deters high-intensity war but allows more risk-taking at lower levels of dispute intensity (George and Smoke 1974). Geographical distance between states appears irrelevant for both types of conflict. Given the rapid spread of the Internet in recent decades, it is not surprising that the distance between two states does not significantly affect the ability of rivals to engage in digital or physical exchanges.

Our findings contribute theoretically to the literature on coercion and apply to policy debates regarding both within- and cross-domain conflict by suggesting that observers may have overestimated the role that COs play in conventional conflict. These findings provide preliminary support for the recent scholarship that views actors' behavior in cyberspace as an "intelligence contest" primarily (Chesney et al. 2020). This study also contributes methodologically. By introducing a novel conceptualization and measure of complementarity and substitutability, we confirm the importance of differentiating between sequential and concurrent effects of cyber and conventional fronts. The approach should perhaps be applied to other areas of international relations and comparative politics.

Our study is not without limitations. Even though our results suggest that digital and conventional fronts are generally independent, this may certainly change as more nations deploy information campaigns alongside war "on the ground." Cyber and conventional operations could also complement (e.g., Russia's use of conventional and COs against Ukraine, the U.S.'s use of conventional and cyber operations against the Islamic States) or substitute over longer intervals (e.g., a delayed U.S. response to the 2014 Sony hack). Moreover, nations have begun a shift in cyber strategies predicated on a greater presence in adversarial networks. Such "defend forward" doctrines might

produce more rapid responses in the future, similar to the 2019 U.S. cyber-attack against Iranian weapons systems in response to the bombing of oil tankers in the Gulf of Oman. Countries might also resort to conventional force in response to COs, as for example when the Israeli Defense Force conducted an air strike against a building said to house a Hamas hacking group accused of mounting cyber attacks against Israel.

While fundamental forces will continue to propel more Internet-dependent nations away from traditional forms of warfare and toward COs, we expect a few individual cases to continue exhibit exceptions from this general trend because countries can get creative with how they achieve their strategic objectives. For instance, the U.S. killing of top Iranian general Qasem Soleimani shows that in certain cases conventional options can be quite useful in the digital era. To limit access to sensitive data, countries will continue air-gapping their computer systems (i.e., making them inaccessible remotely). Some countries may continue prioritizing territorial conquest. But these few outliers do not necessarily suggest that killing of the generals, airgapping all facilities, or conquering sovereign states will become new trends. As a result, these deviant cases are unlikely to change our main theoretical prediction that technologically sophisticated states will continue to compete over information as they pursue their strategic goals.

While we offer only a first stab at understanding how cyber and conventional conflict interact, future research can build on our efforts to investigate how this dynamic alters in different samples, or investigate how different types of COs are being used at different intensities, with different counterparts, during different levels of peace (Diehl, Goertz, and Gallegos 2019). Future research will further benefit by empirically studying a *cross-substitution* scenario in which state A uses COs in a previous period to degrade State B's capabilities to engage in conventional warfare in subsequent period, reducing State B's likelihood of engaging in conventional conflict in this period. Finally, future research will sustain or contradict our findings. We look forward to improvements in data coverage that might allow researchers to more authoritatively assess the nature of cooperation and contestation in the cyber domain. For now, our findings must cast considerable doubt on the rising view that cyber conflict is a complement to conventional forms of conflict.

Acknowledgements

We would like to thank Erica Borghard, Aaron Brantly, Andres Gannon, Susan Landau, Jon Lindsay, Jacquelyn Schneider, Ryan Shandler, Brandon Valeriano, and the participants of the Student Cybersecurity Symposium at the Tufts University, of the Digital Issues Discussion Group. This paper was presented at the 2019 International Studies Association Conference.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Dr. Kostyuk would like to acknowledge The William and Flora Hewlett Foundation for funding this research under award #: 2018-7277. Dr. Gartzke would like to acknowledge The William and Flora Hewlett Foundation for funding this research under award #'s: 2020-1961, 2021-2955. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the view of our sponsors.

ORCID iD

Nadiya Kostyuk https://orcid.org/0000-0003-0596-5752

Supplemental Material

Supplementary materials and replication files available at: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/96DDGF.

Notes

1. *Joint Publication 3 13 Information Operations* (2014, II-9) define "cyber-operations" as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."
2. We use "conventional" and "kinetic" interchangeably in this paper.
3. A plausible analogue could be "air war," such as, for example, the Battle of Britain, during which contestation in a new, previously almost unimaginable domain largely replaced kinetic forms of battle.
4. Standard techniques generally focus only on the sequential development of physical conflict behavior.
5. Evidence from previous research suggests that proximity affects selection into rivalry (Buhaug and Gleditsch 2006).
6. Successful coercion requires that punishment be both anticipated and avoidable by accommodation (Schelling 1966)—two criteria that are difficult to realize in cyberspace. First, COs are most effective when unanticipated, and depreciate quickly after first use. This creates incentives for surprise "zero-day" attacks before the target is aware of a vulnerability. Second, targets may also question whether an adversary can credibly commit to ceasing its attacks, due to attribution problems and uncertainty over an attacker's identity. Targets may also see compliance as unnecessary to prevent further damage, especially once vulnerabilities are known.
7. e.g., *Snake* starting in 2006.
8. Rather than simply being a scope condition, the spread of the Internet actively creates an indirect relationship by increasing the likelihood that a country experiences cyber conflict and decreases the likelihood that the country experiences terrestrial conflict.
9. States with surveillance satellites are less likely to be attacked (Early and Gartzke 2021).

10. As we revise this manuscript, Russia has invaded Ukraine. It appears that the objectives of Russian authorities in conducting a physical invasion of Ukraine have less to do with obtaining information and more to do with more traditional goals, such as political influence and strategic depth. Indeed, the invasion seems to hinge on a worldview that is backward looking and out of step with the new realities of an informational world. Despite that, the flow of information and sustaining government and citizen communication via Internet-connected technologies remain top priorities in this conflict (Kostyuk and Gartzke 2022).
11. It is not surprising that countries continue investing in their armed forces because they serve various functions, and war is only one of them. Unlike these other functions, such as maintaining domestic stability, peacekeeping, coercion of rivals, wars are less fruitful now because (1) they are quite costly; and (2) there are other cheaper ways of obtaining a country's strategic objectives. Given that interstate conflict is the most useful tool for capturing territory, physical conquest generally holds less appeal in the 21st century.
12. Changing objectives and domains are unlikely to be felt equally by all nations, or at the same pace.
13. Since we are interested in studying an effect of an exogeneous variable, a country's Internet access, this relationship is co-occurent in some sense. Thus, we do not distinguish between co-occurrence and sequentiality in these hypotheses.
14. Again, this reality may change as the "internet of things" becomes more widespread, but this was not the case in the time period under study here. Even with the Internet increasingly integrating with the physical world, the ability to control or obstruct physical space through cyberspace will remain limited.
15. Since we are interested in studying an effect of a country's Internet access, we do not distinguish between co-occurrence and sequentiality in these hypotheses.
16. Since the data on COs begins in 2000 and the MIDs dataset extends only until 2010, we focus on the 2000-2010 interval.
17. The Council on Foreign Relations data is much less useful for the purposes of this study because it includes information on only when an attack became public and does not provide information on an attack's start or end dates.
18. This is especially the case when a significant amount of time has passed since the start of an incident—between nine and 19 years for the 2000-2010 period.
19. Despite our confidence in DCID as suitable for this analysis, we run robustness checks that consider the possibility that COs remain under/over-reported in DCID. Our results generally hold (Online Appendix Section 4.1).
20. We exclude events that resulted in "released" because "a seizure of material or personnel" was the main reason for such disputes (Jones, Bremer, and Singer 1996, 180). Our results remain robust even if we included events with this outcome into our analysis.
21. Contiguity is among the most substantive explanations of conventional conflict (i.e., MIDs) between rivals (Senese 2005). The regionalism of cyber-operations—territorial contiguity and not virtual isolation—provides some anecdotal support for complementarity of cyber and conventional fronts, further pointing to the appropriateness of looking at the overlap between MIDs and cyber incidents (Valeriano and Maness 2014). While Valeriano and Maness (2014) only introduce their DCID dataset and provide descriptive statistics of how

likely rivals are to use cyber events, they neither test their theoretical claims empirically nor test how likely rivals are to use cyber along or instead of conventional operations. This is where our research comes in.

22. Previous studies use Internet per capita as a proxy for the state cyber-capacity as well as its vulnerability (Valeriano, Jensen, and Maness 2018). We follow these authors and use this variable to identify a country's Internet access. Importantly, adopting the measure that previous researchers have used allows us to compare our results to those previously obtained and to move the field forward by creating new knowledge on how the spread of the Internet shapes modern warfare.
23. We logarithmized this variable to address its skewness. Our main model does not include GDP per capita because of high correlation of this variable with Internet users per capita (80%). Online Appendix Section 4.8 which presents models with GDP per capita shows that our results remain unchanged.
24. We include dummies for the nuclear-armed states recognized by the Nuclear Non-proliferation Treaty, "unofficial" weapons states, a presumed nuclear weapons state, and the North Atlantic Treaty Organization nuclear weapons sharing state.
25. We use odds ratios to describe associations between different types of conflict and covariates. Odds ratios larger than 1 identify positive correlations and odds ratios between 0 and 1 identify negative correlations.
26. The reason we obtain large odds ratios and confidence intervals for cyber espionage is because these operations tend to last for multiple years, so that there is little variation after accounting for lagged cyber-espionage.
27. We use Model 3 because it has the lowest Akaike Information Criterion (AIC), suggesting the best model fit.
28. We do notrun robustness checks using a temporal dimension lower than a month, given that an average duration of cyber conflict is 134 days and an average duration of conventional conflict is 132 days.

References

Akoto, William. 2021. "International Trade and Cyber Conflict: Decomposing the Effect of Trade on state-Sponsored Cyber Attacks." *Journal of Peace Research* 58: 0022343320964549.

Borghard, Erica D, and Shawn W Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 452-481.

Buhaug, Halvard, and Nils Petter Gleditsch. 2006. "The Death of Distance? The Globalization of Armed Conflict." *Territoriality and Conflict in an Era of Globalization*: 187-216.

Chesney, Robert, Max Smeets, J Rovner, M Warner, JR Lindsay, MP Fischerkeller, RJ Harknett, and N Kollars. 2020. "Policy Roundtable: Cyber Conflict as an Intelligence Contest." *Texas National Security Review* 17.

Clarke, Richard A, and Robert K Knake. 2010. "Cyber War: The Next Threat to National Security and What to Do About It".

Cunningham, Fiona S. 2022. "Strategic Substitution: China's Search for Coercive Leverage in the Information Age." *International Security* 47 (1): 46-92.

De Mesquita, Bruce Bueno, and David Lalman. 1988. "Empirical Support for Systemic and Dyadic Explanations of International Conflict." *World Politics: A Quarterly Journal of International Relations* 41: 1-20.

Diehl, Paul F, Gary Goertz, and Yahve Gallegos. 2019. "Peace Data: Concept, Measurement, Patterns, and Research Agenda." *Conflict Management and Peace Science* 38: 0738894219870288.

Dobson, Melina J. 2020. "Operation Rubicon: Germany as an Intelligence 'Great Power?" *Intelligence and National Security* 35 (5): 608-622.

Early, Bryan R, and Erik Gartzke. 2021. "Spying from Space: Reconnaissance Satellites and Interstate Disputes." *Journal of Conflict Resolution* 65: 1-20.

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organization* 49 (3): 379-414.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41-73.

Gartzke, Erik, and Dominic Rohner. 2011. "The Political Economy of Imperialism, Decolonization and Development." *British Journal of Political Science* 41 (3): 525-556.

Gartzke, Erik, and Jon R. Lindsay. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity.* Oxford: Oxford University Press.

George, Alexander L, and Richard Smoke. 1974. *Deterrence in American Foreign Policy: Theory and Practice*. New York City: Columbia University Press.

Gochman, Charles S, and Zeev Maoz. 1984. "Militarized Interstate Disputes, 1816-1976: Procedures, Patterns, and Insights." *Journal of Conflict Resolution* 28 (4): 585-616.

Gohdes, Anita R, and Sabine C Carey. 2017. "Canaries in a Coal-Mine? What the Killings of Journalists Tell us About Future Repression." *Journal of Peace Research* 54 (2): 157-174.

Henley, Jon. 2021. "Denmark Helped US Spy on Angela Merkel and European Allies – Report." *The Guardian*.

Holsti, Kalevi. 2016. "The Decline of Interstate War: Pondering Systemic Explanations." In *Kalevi Holsti: Major Texts on War, the State, Peace, and International Order*, 43-64. Springer.

Horowitz, Michael C, and Neil Narang. 2014. "Poor Man's Atomic Bomb? Exploring the Relationship Between "Weapons of Mass Destruction"." *Journal of Conflict Resolution* 58 (3):509-535.

Joint Publication 3 13 Information Operations. 2014.

Jones, Daniel M, Stuart A Bremer, and J David Singer. 1996. "Militarized Interstate Disputes, 1816–1992: Rationale, Coding Rules, and Empirical Patterns." *Conflict Management and Peace Science* 15 (2): 163-213.

Karatzogianni, Athina. 2015. *Firebrand Waves of Digital Activism 1994-2014: The Rise and Spread of Hacktivism and Cyberconflict*. New York City: Springer.

Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7-40.

Kostyuk, Nadiya, and Erik Gartzke. 2022. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine (Summer 2022)." *Texas National Security Review.*

Kostyuk, Nadiya, and Yuri M Zhukov. 2019. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63 (2): 317-347.

Liebetrau, Tobias. 2022. "Cyber Conflict Short of War: A European Strategic Vacuum." *European Security* 31: 1-20.

Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401-428.

Maoz, Zeev. 2005. "Dyadic Militarized Interstate Disputes Dataset Version 2.0." *UC Davis*.

Mehta, Rupal N. 2020. *Delaying Doomsday: The Politics of Nuclear Reversal*. USA: Oxford University Press.

Monteiro, Nuno P, and Alexandre Debs. 2014. "The Strategic Logic of Nuclear Proliferation." *International Security* 39 (2): 7-51.

Paul, Thazha V. 2012. "Disarmament Revisited: Is Nuclear Abolition Possible?" *Journal of Strategic Studies* 35 (1): 149-169.

Powell, Robert. 1999. *In the Shadow of Power: States and Strategies in International Politics*. Princeton: Princeton University Press.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5-32.

Sanger, David E. 2012. "Obama Order Sped up Wave of Cyberattacks Against Iran." *The New York Times* 1 (06): 2012.

Schelling, Thomas C. 1966. *Arms and Influence*. New Haven: Yale.

Senese, Paul D. 2005. "Territory, Contiguity, and International Conflict: Assessing a New Joint Explanation." *American Journal of Political Science* 49 (4): 769-779.

Singer, J David, Stuart Bremer, and John Stuckey. 1972. "Capability Distribution, Uncertainty, and Major Power War, 1820-1965." *Peace, War, and Numbers* 19: 48.

Thompson, William, and David Dreyer. 2011. *Handbook of International Rivalries*. Washington D.C.: CQ Press.

Thompson, William R. 2001. "Identifying Rivals and Rivalries in World Politics." *International Studies Quarterly* 45 (4): 557-586.

Valeriano, Brandon, Benjamin Jensen, and Ryan C Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Valeriano, Brandon, and Ryan C Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11." *Journal of Peace Research* 51 (3): 347-360.

Weidmann, Nils B. 2016. "A Closer Look at Reporting Bias in Conflict Event Data." *American Journal of Political Science* 60 (1): 206-218.