Invisible Digital Front:
Can Cyber Attacks Shape Battlefield Events?

Nadiya Kostyuk and Yuri M. Zhukov
University of Michigan

July 12, 2017

Abstract

Recent years have seen growing concern over the use of cyber attacks in wartime, but little evidence that these new tools of coercion can change battlefield events. We present the first quantitative analysis of the relationship between cyber activities and physical violence during war. Using new event data from the armed conflict in Ukraine – and additional data from Syria's civil war – we analyze the dynamics of cyber attacks, and find that such activities have had little or no impact on fighting. In Ukraine – one of the first armed conflicts where both sides deployed such tools extensively – cyber activities failed to compel discernible changes in battlefield behavior. Indeed, hackers on both sides have had difficulty responding to battlefield events, much less shaping them. An analysis of conflict dynamics in Syria produces similar results: the timing of cyber actions is independent of fighting on the ground. Our finding – that cyber attacks are not (yet) effective as tools of coercion in war – has potentially significant implications for other armed conflicts with a digital front.

Word count: [176] (abstract) + [6,853] (main text) + [2,604] (notes, tables) + [1,159] (references) = [10,792]

On December 23rd, 2015, hackers attacked Ukraine's power grid, disabling control systems used to coordinate remote electrical substations, and leaving people in the capital and western part of the country without power for several hours. The Security Service of Ukraine blamed the Russian government for the cyber attack, an accusation that later found support in malware analysis by a private computer security firm. The Ukrainian hack was the first publicly acknowledged case of a cyber attack successfully causing a power outage. It is also just one of thousands of cyber activities, mostly diffuse and low-level, that have occurred alongside physical fighting in Ukraine. Attacks launched through the digital realm are playing an increasingly visible role in civil and interstate conflict – in Ukraine, Syria, Israel, Estonia, Georgia and beyond. Yet it remains unknown whether such activities have a real coercive impact on the battlefield.[1]

Recent years have seen growing concern over the coercive potential of cyber capabilities in war, but little evidence that these new tools are yet making a difference. Theoretically, most research has focused on the consequences of cyber attacks for peacetime deterrence, rather than wartime compellence (Libicki, 2009; Sharma, 2010; Andres, 2012).[2] Yet the logic of

[1] We define *coercion* as an attempt to influence a target's behavior by increasing the costs associated with an unwanted action. *Cyber activities* apply these costs through the disruption, destruction, malicious control, or surveillance of a computing environment or infrastructure (Kissel 2013). *Kinetic* or *physical operations* apply costs through physical force. *Low-level* cyber attacks cause minor disruptions and include web-page defacements, phishing, distributed-denial of service attacks. *High-level* cyber attacks include serious disruption with loss of life and extensive infrastructure disruption.

[2] *Deterrence* seeks to convince a target to not start an unwanted action. *Compellence* seeks to convince the target to stop an ongoing unwanted action.

coercion entails distinct challenges in peace and war, with potentially different implications for the cyber domain. Empirically, the literature has relied more on qualitative case studies than quantitative data. The few datasets that do exist (Valeriano and Maness, 2014) privilege massive cyber catastrophes over less sophisticated low-intensity attacks, like distributed-denial-of-service. The latter category, however, is far more common.

This article asks whether cyber attacks can compel short-term changes in battlefield behavior, using new event data on cyber and kinetic operations from armed conflicts in Ukraine and Syria. We use the Ukrainian conflict as our primary test case due to the extensive and sophisticated use of cyber attacks by both sides (Geers 2015), and – uniquely – overt claims of responsibility, public damage assessments, and other releases of information that reduce uncertainty over timing and attribution. Since 2014, Ukraine has turned into "a training playground for research and development of novel attack techniques" (Zetter, 2017). If cyber attacks can yet make a difference on the battlefield, Ukraine is where we are most likely to observe such an effect. Our data include 1,841 unique cyber attacks and 26,289 kinetic operations by government and pro-rebel forces, between 2014 and 2016. We supplement this quantitative analysis with 14 primary-source interviews with participants in the cyber campaign, as well as Ukrainian, Russian and Western cyber security experts with direct knowledge of these operations.

To evaluate the generalizability of the Ukrainian experience to other conflicts, we replicate our results with data from Syria's civil war. Like

Ukraine, Syria has seen the extensive use of low-level cyber attacks by factions fighting for and against the incumbent regime. Because this war has gone on significantly longer than the conflict in Ukraine – giving hackers more time to organize and develop their capabilities – Syria offers a glimpse at cyber activities in a more protracted, higher-intensity context. If we uncover similar patterns in two conflicts of such different scale and complexity, we can have greater confidence that our results are not artifacts of a single idiosyncratic case. Our data include 682 cyber attacks and 9,282 acts of violence by pro- and anti-Assad forces, between 2011 and 2016.

Evidence from both conflicts suggests that cyber attacks have not created forms of harm and coercion that visibly affect their targets' actions. Short of mounting synchronized, coordinated cyber campaigns, each group of hackers has seemed to operate in its own 'bubble,' disengaged from unfolding events in both cyberspace and the physical world. The lack of discernible reciprocity between cyber and kinetic operations – and between the cyber actors themselves – questions whether cyber attacks can (yet) be successfully deployed in support of military operations.

This disconnect may be temporary, as joint planning and execution concepts continue to evolve. Many countries, for instance, still struggle in coordinating airpower for ground combat support, a century after World War I. Our study highlights some of the difficulties that countries will need to overcome in integrating and synchronizing these new capabilities.

Our contribution is fourfold. We offer the first disaggregated analysis of

cyber activities in war, and take stock of the empirical relationship between the cyber and kinetic dimensions of modern battle. To do so, we collect the first micro-level data on wartime cyber attacks, using both open media sources and anonymous attack traffic data. Theoretically, our analysis addresses an important question on the coercive impact of low-level cyber attacks, advancing a literature that has been heavy on deductive argumentation, but light on evidence. Finally, from a policy standpoint, our findings should temper the popular tendency to overhype the transformative potential of cyber attacks. At present, interaction between cyber and kinetic operations is similar to that between air power and ground operations in World War I – when armies began to use aircraft for reconnaissance, but had not realized their full potential to shape battlefield outcomes.

Varieties of Cyber Activity

The term 'cyber activities' captures a diverse assortment of tactics and procedures, directed against different types of targets, in pursuit of disparate objectives. Not all of these activities seek to achieve battlefield effects in the same way. Before proceeding further, we differentiate between two broad goals these actions tend to pursue: propaganda and disruption.[3]

Cyber activities in the propaganda category seek to influence public opinion, and indirectly undermine an opponent's financing or recruitment.

[3] We use *cyber propaganda* when referring to the propaganda category, *cyber attacks* when referring to disruption (Cartwright and James, 2010), and *hybrid cyber operations* when referring to hybrids of the two.

Operations in this group include leaks of compromising private information, online publication of partisan content (e.g. "trolling" on comments pages), and the establishment of dedicated websites and forums to promote an armed group's message. Unless it openly incites or discourages violence, propaganda affects kinetic operations only indirectly, by undermining an opponent's support base, or obfuscating perceptions of events.

In the Ukrainian conflict, the importance both groups attach to online propaganda is evident from the time and resources pro-Kyiv fighters spend updating Wikipedia, and pro-Russia groups devote to creating and running dedicated YouTube channels and social media accounts. Russian military doctrine places a heavy emphasis on the strategic use of information in warfare, as does U.S. cyberspace joint planning doctrine.

The second category of cyber attacks – disruption – seeks to directly sabotage opponents' ability to operate in the physical or electronic realm. These mostly low-intensity activities include denial of service (DOS) attacks, which make targeted resources unavailable through a flood of requests from a single source, and distributed denial of service (DDoS) attacks, where requests originate from multiple compromised systems. Related efforts include inundating communications systems with floods of text messages or phone calls, and using firewalls and proxies to block access to websites. At the extreme end of the scale is the use of malicious code to inflict physical damage or otherwise compromise infrastructure and military objects. Examples include interception of drones, communica-

tions and surveillance systems, control of WiFi access points, and collection of protected information via phishing.

The most sophisticated known attack of this type is the Stuxnet worm, which – before its discovery in 2010 – targeted industrial control systems critical to uranium enrichment in Iran. In Ukraine, notable disruptive activities have included attacks on the Central Election Committee's website during the 2014 presidential elections, and attacks on the country's electrical power grid in 2015 and 2016. Other examples include the use of malware to collect operational intelligence, like X-Agent, which retrieved locational data from mobile devices used by Ukrainian artillery troops (CrowdStrike, 2016), and the hacking of CCTV cameras behind enemy lines.

Propaganda and disruption are not mutually exclusive, and many cyber activities serve both purposes simultaneously – shaping public opinion through disruption, or disrupting an opponent's operations by shaping public opinion. For example, altering the visual appearance of websites can have the dual effect of embarrassing the target and limiting its ability to communicate. Leaks of private information can also have dual implications for targets' public image and physical security.

Recent examples of hybrid activities include the defacement of U.S. Central Command's Twitter and Facebook pages by the Islamic State's (IS) Cyber Caliphate, and operations by U.S. Cyber Command against IS beginning in April 2016. In Ukraine, the pro-rebel group CyberBerkut has leaked private communications from senior U.S., EU and Ukrainian officials, and

disclosed the identities of pro-Kyiv field commanders – simultaneously creating a media scandal and forcing targets to commit more resources to their own security. Similarly, the pro-Kyiv website *Myrotvorets'* published names and addresses for thousands of suspected 'rebel sympathizers' – information that allegedly facilitated several assassinations (Il'chenko, 2016).

In the following, we limit the scope of our inquiry to cyber actions that are either purely disruptive (e.g., DDoS-style attacks) or are hybrids of the two approaches (e.g., web defacements). We do so for two reasons. First, most purely propagandistic operations, like comment-board "trolling," do not aspire to influence the course of military operations in the short term. Second, it is hard to separate the disruptive and propaganda effects of hybrid cyber activities, because they depend on each other.

Cyber Coercion in Wartime

Over the last two decades, cyber attacks have become an increasingly common tool of coercion, used by state and non-state actors, independently and jointly with physical, kinetic operations. Like other instruments of coercion, cyber actions inflict costs on a target to compel a change in its behavior – either by punishing past misdeeds, or by putting pressure on decision-makers in real time.

The role of cyber compellence in wartime is not unlike that of air power or terrorism (Pape, 2003, 2014). Cyber attacks cannot take or hold territory

on their own, but they can support operations on the ground by disrupting opponents' command and control, collecting operational intelligence and creating opportunities for conventional forces to exploit. If combatants use the internet for coordination, recruitment or training, low-level cyber disruption may prevent them from running these vital functions smoothly.[4] Alternatively, cyber attacks can indirectly pressure an opponent by targeting civilian economy and infrastructure, similarly to strategic bombing. Yet unlike air power, an operational cyber capability is relatively inexpensive to develop. It does not require new massive infrastructure, and many activities can be delegated to third parties (Ottis, 2010). Unlike terrorism, the individual attacker is rarely at risk of direct physical harm.

Despite the apparent promise of these "weapons of the future" (Schmitt, 1999; Rios, 2009; Clarke and Knake, 2010; McGraw, 2013; Eun and Aßmann, 2014), some scholars have remained skeptical that low-level cyber attacks can be an effective tool of coercion (Liff, 2012; Rid, 2012; Gartzke, 2013; Junio, 2013). There is little doubt that large numbers of low-level attacks can cumulatively produce large-scale damage, bringing "death by a thousand cuts" (Lemay, Fernandeza and Knight, 2010). Yet successful coercion also requires punishment to be both anticipated and avoidable (Schelling 1966), and these criteria can be difficult to meet in cyberspace.

Cyber attacks can be challenging for targets to anticipate because attack-

[4] For example, U.S. Cyber Command has used low-level cyber operations to "disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and [pay] its fighters" (Sanger, 2016).

ers face strong incentives to mount surprise "zero-day" exploits, before targets recognize and patch their vulnerabilities (Axelrod and Iliev 2014).[5] Since the destructiveness of malicious code depreciates quickly after first use, cyber attacks are often most damaging when they are least anticipated.

Targets also have many reasons to doubt that cyber attacks are avoidable by accommodation. For the attacker, cyber actions present a trade-off between plausible deniability – which helps prevent retaliation – and the credibility of coercive promises and threats.[6] Any uncertainty over the source of an attack will also create uncertainty over the nature of compliance – what sort of actions will prevent future attacks, and by whom.

Beyond attribution uncertainty, cyber attacks may not generate sufficient costs to elicit compliance from the target. Because administrators can quickly fix or contain many exploited vulnerabilities, even successful cyber attacks cause only temporary disruption (Axelrod and Iliev 2014). Unless the attacker continues to develop new methods and identify new vulnerabilities, a protracted campaign may quickly lose its coercive impact. As a result, targets may see compliance as both insufficient and unnecessary to stop the damage (Hare, 2012; Lynn, 2010; Nye Jr, 2010).

Force synchronization challenges may also render the timing of cyber attacks suboptimal for compellence. Hackers – especially those not integrated with military forces – may not observe battlefield events on a tac-

[5] A *zero day vulnerability* is a security hole previously unknown to the target.

[6] This trade-off is not unique to the cyber domain. In civil conflict, for example, pro-government militias pose a similar dilemma for state repression (Gohdes and Carey, 2017).

tically relevant timeline. Even if they did, 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.

These challenges are not insurmountable. Lead time is a greater barrier for high-level attacks (e.g. targeting major infrastructure) than for more routine, DDoS-style attacks. Force synchronization difficulties are also not unique to the cyber domain, and are well-established in research on terrorism and air power (Atran, 2003; Pape, 2003, 2014). The ability of contemporary hackers to overcome these difficulties, however, remains unknown.

Previous research

The question of whether low-level cyber attacks compel has deep implications for the theory and practice of national security. Yet the public and academic debate on this topic has unfolded largely in the absence of rigorous empirical evidence in either direction. Existing political science and policy literature on cybersecurity could be grouped into three broad areas: the "big picture" of cyber warfare (Cha, 2000; Griniaiev, 2004; Libicki, 2007, 2011; Czosseck and Geers, 2009; Clarke and Knake, 2010; Axelrod and Iliev, 2014); the overlap between cyber and kinetic capabilities (Healey, 2013; Kello, 2013; Libicki, 2015; Andress and Winterfeld, 2013; Axelrod, 2014); and the effect of information and communication technology (ICT) on conflict (Martin-Shields, 2013; Pierskalla and Hollenbach, 2013;

Crabtree, Darmofal and Kern, 2014; Gohdes, 2014; Bailard, 2015).

Most research in the first category has focused on the implications of cyber activities for peacetime deterrence or the offense-defense balance, rather than wartime compellence. While the second group focuses more directly on cyber attacks during conflict, its empirical approach has been mostly qualitative, relying on evidence from descriptive case studies, macro-historical surveys and stylized facts. Some large-n analyses do exist (Valeriano and Maness, 2014), but their scope has remained on large-scale cyber attacks, rather than the far more numerous low-intensity operations we consider here. While the third group does employ the statistical analysis of disaggregated data, its theoretical scope is distinct from mainstream literature on cyber attacks – evaluating, for instance, how technology affects collective action (Weidmann 2015), rather than military compellence.

Our study bridges the gap between these areas of inquiry. Our goal is to assess the coercive potential of low-level cyber actions during an armed conflict. We pursue this goal by studying the magnitude and direction of the relationship between cyber attacks and physical violence, using micro-level data from ongoing conflicts in Ukraine and Syria.

Empirical expectations

Cyber attacks by actor A can affect physical violence by B in one of three ways: negatively, positively or not at all. If cyber compellence is successful, we should expect a short-term decrease in violence after a spike in cyber

attacks. A positive response would suggest failure, where cyber attacks actually escalate violence by the opponent. If no relationship exists, cyber actions are either ineffective or irrelevant to fighting in the physical world.

In addition to compellence across domains, cyber attacks by actor A may also impact cyber attacks by actor B. As before, only a negative relationship would imply coercive success, while a null or positive response would suggest that these actions are either ineffective or counter-productive.

Data Analysis

To evaluate whether and how cyber actions affect physical violence in war, we analyze new micro-level data from Ukraine and Syria. We begin with an in-depth study of the Ukrainian case, as a "most likely test" of cyber coercion. Due to the sophistication of hackers on both sides, the public nature of many attacks, and an abundance of data, the Ukrainian conflict is one where cyber attacks are most likely to have an observable coercive effect.[7] If we fail to find such relationship in Ukraine, we can reasonably expect similar results to hold elsewhere. We then use analogous event data on Syria to evaluate the generalizability of our results.

[7] Although a case study of the Russian-Georgian War of 2008 could also have been illuminating, its short conflict-duration (five days) complicates analysis, for three reasons. First is the lack of sufficient variation of cyber attacks over this abbreviated period. Second is the difficulty of differentiating the 'cyber effect' from the near-simulataneous effects of conventional military operations. Third is the problem of generalizability: its five-day duration is an extreme outlier among interstate and civil wars (interstate wars, on average, tend to last a few years; the average civil war lasts between seven and twelve years post 1945).

In assembling our data, we followed two general guidelines. To address systematic differences in event reporting cross countries and media outlets (Baum and Zhukov, 2015; Davenport and Stam, 2006; Woolley, 2000), we drew data from multiple open sources – including press reports and anonymous attack traffic data. To reduce potential false positives, we included only those events that have been reported by more than one source.[8]

Ukraine Cyber Attacks Data

Our cyber event data on Ukraine include 1,841 unique, mostly low-level, cyber attacks from 27 August 2013 to 29 February 2016, drawn from two sets of sources. First are media reports of cyber attacks from rebel, Russian, Ukrainian, and Western news outlets, press releases and blogs, along with social media platforms used by the involved non-state actors.[9] Second is the private cyber security firm Arbor Networks' Digital Attack Map (DAM).[10] Unlike media sources – which include only cyber attacks publicly reported by news organizations, or claimed by governments and hacker groups directly – DAM draws on anonymous attack traffic data and network outage reports to enumerate the top 2% of reported attacks that generate unusually high internet traffic for each country. Including these

[8] Sections 3.1 and 3.2 along with the Online Appendix provide an overview of these sources.

[9] Rebel sources include *Donetsk News Agency*. Russian sources include *RIA Novosti, Sputnik*, and *Vesti.ru*. Ukrainian sources include *Interfax Ukraine, Segodnya*, and *RBK-Ukraina*. Western sources include technical (*Arstechnica, Digital Dao, Information Week, F-Secure, Graham Cluley, TechWeek Europe*) and mainstream news (*Die Welt, Newsweek, New York Times, Politico, Postimees (Estonia), Security Affairs, The Christian Science Monitor*).

[10] http://www.digitalattackmap.com/about/

"higher-visibility" attacks should make it easier to find a coercive effect.

We supplemented these data with 14 primary-source interviews with participants in the cyber campaign, as well as Russian, Ukrainian, and Western cyber security experts with direct knowledge of these operations, from the private and public sectors, academia, and journalism.[11] We conducted all interviews in person or via email or Skype in the summer and fall of 2015, and provide full transcripts in the appendix (Interviews 2015).

We grouped cyber attacks in our dataset according to the partisanship of alleged perpetrators (pro-Ukrainian vs. pro-rebel), and the type of operation they conducted (propaganda vs. disruption). Table 1 list all actors conducting cyber activitiess in the Ukrainian conflict, their targets, and the reported frequency of their activities.

Ukrainian cyber actions include specific attacks by pro-Kyiv hackers, like Anonymous Ukraine and Ukrainian Cyber Forces (UCF). The latter is the most active group on the pro-Ukrainian side. In an interview, UCF leader Eugene Dokukin claimed to have established the non-state group in March 2014, in response to Russian cyber attacks. Due to the 'secret nature' of the organization, Dokukin was reluctant to discuss its size, but noted that

[11] Our Ukrainian interviewees included experts from the Ukrainian Cyber Forces, CERT-UA, *StopFake, InfoPulse, Luxoft, Berezha Security*, Open Ukraine Foundation, and the Ukrainian Central Election Committee. Western experts' affiliations include New York University, Chatham House, the Center for Strategic and International Studies, RAND Corporation, *The Economist, Mashable*, New America Foundation, and the NATO Cyber Center of Excellence. Due to the complicated political situation in Russia at the time, many of our contacts there refused to speak on record, with the exception of a journalist from *Agentura.ru*. However, many Western interviewees have lived in Russia, speak the language, and are knowledgeable on Russia's information security issues.

the number of volunteers fluctuates depending on the state of kinetic operations in eastern Ukraine (Interviews 2015: # 1). Pro-Kyiv hackers' most common targets are the communications and finances of rebel units, media firms and private companies in rebel-held areas.

Pro-rebel cyber actions include specific attacks by pro-separatist or pro-Russian cyber actors, like CyberBerkut (CB), Cyber Riot Novorossiya, Green Dragon, and the Russian government. The first of these takes its name from Ukraine's disbanded Berkut riot police, and claims to fight "neo-fascism" in Ukraine. Ukrainian and Russian cyber experts we interviewed offered contradictory assessments on CB's organizational structure. One Russian expert said that CB consists of former Security Service of Ukraine (SBU) employees who lost their jobs after the Euromaidan revolution (Interviews 2015: # 12). Contrarily, Ukrainian interviewees viewed CB either as a virtual group controlled by the Federal Security Service (FSB) or as a unit within the FSB (Interviews 2015: #7 & #8). These groups' most popular targets include Ukrainian government officials, media and private citizens.

We further disaggregated these events into the two categories previously defined – propaganda or disruption – as well as a third, hybrid, category of incidents that potentially serve both purposes. The most common cyber actions in Ukraine have been DDoS-style attacks, followed by hacks of CCTV cameras and other communications. Website blockages have also proven popular, as have spear-phishing emails targeting specific individuals. Table 2 provides a breakdown by type and frequency.

To reduce false positives due to unconfirmed reports or dubious claims of responsibility, we only include attacks reported by more than one source. To account for uncertainty of attribution, we marked as "disputed" all cases where no one claimed responsibility, and labeled as "non-disputed" those operations for which actors directly claimed responsibility in press releases, on social media, or in interviews.[12] To focus on daily dynamics, we excluded activities whose intensity did not vary over time.[13]

Figure 1a depicts the temporal dynamics of pro-Ukrainian (Cyber U) and pro-Russian rebel (Cyber R) cyber operations.[14] In early March 2014, about a week after the revolution in Kyiv, Figure 1a shows a spike in attacks by CyberBerkut. The same month saw the establishment of the pro-Kyiv Ukrainian Cyber Forces, partly in response to CB's attacks. However, UCF operations do not become visible until May 2014, following an influx of volunteers to the group. May 2014 is also notable for a rise in activities by another pro-Russian cyber group, Cyber Riot Novorossiya – named after

[12] This is a very conservative standard of attribution, since it includes only direct claims of responsibility, and not accusations by others – even if the latter are substantiated by evidence. For instance, we marked as "disputed" the cyberespionage operation *Armageddon* – which multiple governments and private security firms have attributed to the Russian state – because Moscow never claimed responsibility.

[13] Excluded operations included the malware *Blackenergy*, first launched by Quedagh in 2010; *Operation Potao Express*, a targeted espionage campaign launched in 2011 against the Ukrainian government, military, and news agencies; and *Snake*, a cyberespionage campaign against Ukrainian computer systems.

[14] We aggregated these data to daily time series because geo-location is not possible. Although some individual cyber attacks could, in theory, be tracked to their targets, they represent a small proportion of events. As a result, our cyber data are national-level time series. Even if we could geo-locate all targets of cyber attacks, the diffuse nature of the target set makes spatial matching difficult – servers do not need to be physically located in the warzone for service disruptions to have an effect in the warzone.

the czarist-era term ("New Russia") for territories in southeastern Ukraine. After the first Minsk ceasefire agreement in September 2014, operations by pro-Ukrainian hackers converge to a steady rate of two to four per day, with occasional flare-ups, as in December 2014. Activities by pro-Russian hackers, by contrast, declined after the summer of 2014.

Ukraine Violent Events Data

Our data on kinetic operations include 26,289 violent events from Ukraine's Donbas region, recorded between February 28, 2014 and February 29, 2016. To offset reporting biases in any one source, while guarding against potential disruptions in media coverage due to cyber attacks, these data draw on seventeen Ukrainian, Russian, rebel, and international sources.[15] As before, we include only events that appeared in more than one source.

To extract information on dates, locations, participants, and other event details, we relied on a combination of supervised machine learning (Support Vector Machine) and dictionary-based coding. The online appendix describes our measurement strategy and provides summary statistics.

[15] Ukrainian sources include *Channel 5*, *Espresso.tv*, *Information Resistance*, *112 Ukraina*, and the newswire services *Interfax-Ukraine* and *Ukrinform*. Russian sources include the state-owned television news channel *Russia-24*, the independent TV station *Dozhd*, non-government news websites *Gazeta.ru*, *Lenta.ru* and *BFM.ru*, and the *Interfax* newswire service. Pro-rebel sources include *Donetsk News Agency*, *NewsFront*, *Rusvesna.su*. Also included are the Russian-language edition of Wikipedia, and daily briefings from the OSCE Special Monitoring Mission to Ukraine. Since these are mostly online resources, cyber disruptions can potentially cause under-reporting of violence. Our approach helps ensure that if, for instance, a Ukrainian media firms' servers went down, information could still reach the outside world through one of the sixteen other sources. While unlikely, such endogenous disruptions should increase our chances of finding a coercive cyber effect.

Figure 1b shows the temporal distribution of pro-Ukrainian (Kinetic U) and pro-Russian rebel (Kinetic R) physical violence. The plot shows several notable flare-ups of fighting – during a government offensive in late June 2014, and a rebel offensive in January 2015 – as well as lulls following ceasefire agreements in September 2014, February 2015 and September 2015. Compared to the cyber operations in Figure 1a, this plot reveals a clear correlation between kinetic operations by the two sides, with government and rebel attacks rising and falling in tandem.[16] Although this interdependence is not surprising, the data suggest that – with few exceptions – physical violence in Ukraine has been a reciprocal affair.

From a brief glance at the timing of cyber and physical operations (Figures 1a and 1b), there are relatively few signs of a compellence effect – changes in the former do not appear to drive changes in the latter. However, a visual comparison can be misleading. Some of the variation may be due to fighting on the ground or in cyberspace, but other changes may reflect secular trends or shocks due to elections and other events not directly related to conflict. To account for these potential confounding factors, and to gauge whether there is a stronger cyber-kinetic relationship than we would expect by chance, we conduct a series of more rigorous tests.

[16] Because geo-location is not possible for cyber attacks, we aggregate the physical violence data to daily time series to merge and analyze the datasets.

Empirical Strategy

To evaluate the relationship between cyber and kinetic operations in Ukraine, we estimate a series of vector autoregressive models[17]

$$Y_t = \sum_{j}^{p} B_j Y_{t-j} + GX_t + \mu_0 + \mu_1 t + \epsilon_t \tag{1}$$

where $Y_t = \left[y_t^{\text{Kinetic (U)}}, y_t^{\text{Kinetic (R)}}, y_t^{\text{Cyber (U)}}, y_t^{\text{Cyber (R)}}\right]'$ is a matrix of endogenous variables, and $X_t = [x_{1t}, \ldots, x_{kt}]'$ is a matrix of k exogenous variables, which includes indicators for key dates and events during the war, like presidential and parliamentary electoral campaigns in Ukraine and breakaway territories, ceasefire agreements, and Ukrainian, Russian and Soviet holidays. Deterministic components include a constant term (μ_0) and trend ($\mu_1 t$). p is the lag order, selected via Bayesian Information Criterion, and ϵ_t is a vector of serially uncorrelated errors.

We controlled for Ukrainian, Russian and Soviet holidays because anecdotal accounts suggest significant increases in cyber activity during such times. The UCF, for instance, had an operation called "Happy New Year," which sought to print pro-Ukrainian messages from hacked printers in Crimea, Russia, and Donbas. National election campaigns represent another time when such activities may spike. Before and during the presiden-

[17] Vector autoregression is a common method to study interdependence among multiple time series in economics and political science. Previous applications to conflict research include studies of reciprocity in civil conflicts (Pevehouse and Goldstein, 1999), and the dynamics of terrorism (Enders and Sandler, 2000; Bejan and Parkin, 2015).

tial elections, for instance, hackers bombarded Ukraine's Central Electoral Committee website with DDoS attacks. Finally, we may expect ceasefire agreements aimed at reducing physical violence to also have an effect in the cyber domain. For example, the cyber espionage operation "Armageddon" – directed against Ukrainian government websites – intensified before the Minsk I agreement went into force, but rapidly declined afterward.

Because we are interested in the relationship between cyber attacks and physical violence during war, we limit our primary analysis to the active phase of military operations between May 11, 2014 and February 15, 2015 – the period following independence referendums organized by the self-proclaimed Donetsk and Luhansk People's Republics (DNR, LNR) and the second Minsk ceasefire agreement. In the online appendix, we present additional analyses of the full dataset, which produced similar results.

Results

Data from Ukraine support the skeptical view of cyber coercion. The impulse-response curves in Figure 2 show a strong, escalatory dynamic between kinetic operations by the two sides (Kinetic U, Kinetic R), but no tangible links in either direction between kinetic and cyber operations, and no reciprocity between cyber actions (Cyber U, Cyber R).

Following a standard deviation increase in kinetic rebel attacks, government violence sees a delayed rise, peaking around 2 days after the shock and gradually declining back to zero (top row, second column). Rebel op-

erations also rise after shocks to government operations (second row, first column), but the response here is immediate, without the delay we observe in government operations. This pattern may reflect command and control inefficiencies in the Ukrainian army, particularly early in the conflict, when indecision and leadership turnover lengthened decision cycles.

The relationship between cyber and kinetic operations is far weaker than that between rebel and government violence on the ground. Cyber attacks by pro-Ukrainian forces see no increase after shocks in kinetic government operations, and a positive, but uncertain increase after shocks in kinetic rebel operations (third row, first and second columns).

There is even less evidence that cyber attacks drive kinetic operations. The impulse-response function (IRF) curve for pro-Ukrainian government violence is, in fact, negative after shocks to rebel cyber operations (top row, two rightmost columns). Although this negative response might otherwise suggest that cyber attacks compel a decline in violence – consistent with coercive success – the estimate is also highly uncertain. Following shocks to pro-Ukrainian cyber activities, meanwhile, the main change in rebel kinetic operations is a short-term increase in volatility (second row, third column). Taken together, the data suggest that cyber attacks may make violence less predictable, but do not systematically change its intensity.

Perhaps most surprisingly, there is little or no apparent strategic interaction between 'cyber-warriors' on each side of the conflict. A shock in pro-Ukrainian cyber attacks yields no discernible change in pro-rebel cy-

ber attacks (bottom row, third column) and vice versa (third row, fourth column). The two cyber campaigns, the data suggest, have unfolded independently of each other, and independently of events on the ground.

As the diagonal elements in Figure 2 suggest, there is strong autocorrelation in each time series. For each of the four categories, past shocks in operations yield a significant spike in subsequent operations. To evaluate whether the other categories of events can help us predict future values of each series, after we take this auto-correlation into account, Table 3 reports the results of Granger causality tests. These tests confirm that past levels of pro-rebel and pro-Kyiv kinetic operations help predict each other's future values. Kinetic operations, however, do not appear to "Granger cause" – or be "Granger caused" by – cyber attacks on either side.

Table 4 reports the forecasting error variance decomposition, representing the proportion of variation in each series (rows) due to shocks in each endogenous variable (columns). For most variables, their own time series account for almost all variation at the outset, but this dependency gradually decreases. As before, there is far more dependence within kinetic operations than between kinetic and cyber, or within cyber actions. By the 30 day point in the daily time series, shocks in rebel attacks account for 7 percent of variation in Ukrainian government operations, while shocks in government operations explain 12 percent of variation in rebel violence.

By contrast, shocks to cyber activities account for very little variation in kinetic operations. The highest value is for pro-Russian rebel cyber activ-

ities, which account for 2 percent of short-term variation in government violence. Cyber attacks by each side also have a relatively small impact on each other. Indeed, rebel kinetic operations explain more of the variation in cyber attacks by each actor, than do cyber attacks by the other side.

In sum, our analysis suggests that low-level cyber attacks in Ukraine have had no effect on the timing of physical violence. Not only is there no evidence that cyber attacks have compelled opponents to de-escalate fighting, there is no discernible reciprocity between the cyber actors themselves. Each group of hackers seems to operate in its own 'bubble,' disengaged from unfolding events in both cyberspace and the physical world.

Robustness checks

To gauge the sensitivity of our results to various modeling and measurement choices, we conducted extensive robustness checks. We summarize their results briefly here (Table 5), and more fully in the online appendix.

The first set of tests considers VAR models with alternative orderings of the four endogenous variables, which affects estimation of impulse responses. We find no substantive differences across the 24 permutations.

In a second set of robustness checks, we account for systematic differences in the kinds of conflict events that Ukrainian and Russian media report, which may bias statistical estimates – for example, by underreporting violence by a given actor. Using kinetic data from exclusively Russian or exclusively Ukrainian sources does not change the results.

A third set of robustness tests examines different subsets of cyber attacks. Because purely disruptive activities may impose greater immediate costs than quasi-propagandistic hybrid attacks, pooling these events may dilute their coercive effect. Our results are consistent for all three subsets.

The last set of robustness checks examines different time periods of the conflict, since some cyber attacks pre-dated military activity. In particular, we compare the period of intense fighting previously analyzed (May 11, 2014 to February 15, 2015) to the entire date range for which we have data (February 28, 2014 to February 29, 2016). Our results remain unchanged.

Evidence from Interviews

In interviews, Russian and Ukrainian cyber security experts highlighted five potential explanations for the apparent failure of cyber coercion in Ukraine: (1) lack of resources, (2) lack of coordination, (3) lack of targets, (4) lack of audience, and (5) lack of effort.

The first explanation for coercive failure emphasizes limited resources and capabilities, particularly for the Ukrainian government. Ten years ago, the Security Service of Ukraine (SBU) briefly had a cyber department, but shut it down after a year (Interviews 2015: #3). This unit has recently re-opened, but continues to lack funding and personnel (Interviews 2015: #3, #9). It is possible that, with adequate resources, capabilities and human capital, the Ukrainian cyber campaign might have been more effec-

tive. Resource constraints, however, do not explain coercive failure on the pro-Russian side, where investment in cyber capabilities is more robust.

A second explanation is lack of government coordination with hackers, especially in Kyiv (Maurer and Geers 2015). UCF founder Eugene Dokukin claims to regularly provide the SBU with intelligence from hacked CCTV cameras and has offered cooperation in the past, with no success (Interviews 2015: #1). The SBU's lack of desire to cooperate with the UCF could be due to the illegality of the latter's activities, or the low priority the SBU assigns to cyber actions in the first place (Interviews 2015: #1, #3, #9). Yet again, this explanation is less plausible on the pro-Russian side, where the Kremlin has cultivated extensive ties with non-state hacktivists.

A third explanation is that – even with requisite capabilities and coordination – there are few opportune targets for disruption in Ukraine. Most industrial control systems that run Ukraine's critical infrastructure – particularly its Soviet-era components – are offline, making remote access difficult (Geers 2015, Interviews 2015: #3, #13). Yet some experts disagreed, noting that "weakness of infrastructure [security] should have provoked a DDoS attack" (Interviews 2015: #11). The 2015 and 2016 hacks of Ukraine's power grid also seem to challenge this explanation.

The peculiarities of Ukraine's online population represent a fourth explanation for the indecisiveness of cyber attacks. Since only 44.1% of Ukrainians have internet access – compared to 88.5% in the United States and

71.3% in Russia[18] – and most use it only for social media, a low-level cyber attack that blocks or defaces government websites is unlikely to influence the masses (Interviews 2015: #3). Some experts speculated that this online population pays more attention to purely propagandistic campaigns than disruptive ones (Interviews 2015: #7, #11). Our data suggest that, even if this were the case, propagandistic attacks still had no effect on violence.

The final explanation is that cyber compellence failed because it was never seriously attempted. At first, our interviews with individual hackers revealed no shortage of coercive intent. UCF leader Eugene Dokukin claimed to conduct low-level attacks daily, and vowed to continue until pro-Russian rebels lay down their arms. Dokukin further insisted – contrary to our findings – that there is close coordination between Russia's cyber and kinetic campaigns (Interviews 2015: #1).

While UCF and other non-state groups have explicitly sought to affect battlefield outcomes, some interviewees questioned whether this intent extended to the Russian government. Since Ukraine's information and telecommunication networks generally use Russian hardware and software, Moscow can monitor its neighbor with assets already in place (Interviews 2015: #5, #12).[19] This access, along with vigorous cyber-espionage – some of it ongoing since 2010 – may create incentives against more aggressive actions, which could compromise valuable sources of intelligence.

[18] http://www.internetlivestats.com/internet-users-by-country/.

[19] An example is Russia's *Sistema operativno-rozysknykh meropriyatiy* [System for Operational Investigative Activities], which searches and monitors electronic communications.

Consistent with the 'lack of effort' explanation, some experts noted a shift in Russia's broader cyber strategy, away from disruption and toward propaganda (Interviews 2015: #11). When in 2011 Vyacheslav Volodin replaced Vladislav Surkov as head of the Presidential Administration, he toughened existing laws against Russia's opposition and promoted the use of mass media and online platforms – tools already mostly under state control – to conduct information campaigns. If Russia's cyber activities have shifted toward propaganda due to this strategy change, weak short-term battlefield effects should not be surprising (Interviews 2015: #2, #14).

Evidence beyond Ukraine: Syria's digital front

According to evidence from micro-level data and interviews, cyber attacks did not affect battlefield events in Ukraine. During one of the first armed conflicts where both sides used low-level cyber actions extensively, events in the digital realm have unfolded independently of – and have had no discernible effect on – events on the ground. Conditions in Ukraine were in many ways optimal to observe the coercive impact of cyber actions, for reasons we already discussed (i.e. visibility of major attacks, regular claims of responsibility, less uncertainty over attribution). Yet we found no evidence that low-level cyber attacks affected physical violence. Nor did hackers on each side even affect each other's activities.

While important, Ukraine is not the only contemporary conflict with a

significant cyber dimension. In Syria, state and non-state actors have employed low-level cyber actions extensively for propaganda and disruption, complementing traditional tools of warfare in the deadliest conflict ongoing today. Syria's war has also lasted three years longer than Ukraine's. Over this time, its digital front has expanded in scope and sophistication, offering a glimpse of cyber coercion in a more protracted setting.

An in-depth study of Syria's digital front lies beyond the scope of this paper. A brief analysis of the data, however, suggests that our findings from Ukraine may be part of a broader pattern: cyber capabilities have not yet evolved to the point of having an impact on physical violence.

To evaluate the effectiveness of cyber compellence in this second case, we replicated the model in (Eq. 1), using an analogous daily time series of cyber attacks and violent events in Syria. Our data comprise 9,282 kinetic and 682 low-level cyber attacks, ranging from March 2011 until July 2016.[20] Table 2 provides a break-down of cyber techniques used in the Syrian conflict, their brief description and frequency.[21] Our data on kinetic operations rely on human-assisted machine coding of event reports from

[20] Sources of cyber operations include social media accounts of *Anonymous* or *Anonymous*-supported groups (e.g., *New World Hacking*); *Syrian Electronic Army's* social media accounts; reports by tech companies (e.g., *Risk Based Security, Electronic Frontier Foundation*; computer-security news sources, including *Graham Cluley, TechWeek Europe, Arstechnica, Information Week, Digital Dao, Computer Weekly, Tech News, Wired, Security Affairs*; Middle Eastern mass media sources (e.g., *Turkish News, Arabiya, Doha News*; Russian mass media and social media (e.g., *RT.com, Yahoo.com*); and Western news sources (e.g., *Security Affairs, The Christian Science Monitor, Politico, Die Welt, Reuters, International Business Times, Mashable, Washington Times, The Guardian, BBC*, etc).

[21] Since propaganda operations are not a major focus of our paper, we collected only a small sample of such events during the Syrian conflict.

the IISS Armed Conflict Database (see online appendix for details).

Given the complex nature of the Syrian conflict and the multiple parties involved, we restrict our analysis only to operations by pro-government forces (i.e. Syrian Army, Hezbollah and pro-Assad militias) and the main rebel opposition (i.e. Free Syrian Army, Jaish al-Fatah, including Al Nusra Front). Table 1 provides a list of cyber actors in the Syrian conflict, their targets, and frequency of their activities.

The dynamics of cyber and kinetic operations in Syria exhibit similar patterns to what we saw in Ukraine. Raw data (Figures 3a-3b) suggest relatively little overlap in timing, especially at the beginning of the conflict. The IRF curves in Figure 4 show a rise in rebel operations following shocks to government operations (second row, first column), and mostly negligible (though negative) links between cyber and kinetic operations, and across cyber attacks by each actor. Links between kinetic operations – and their disconnect from cyber attacks – are also evident in variance decomposition results, and Granger tests, provided in the Online Appendix.

There are several reasons for caution in interpreting these results. The Syrian conflict involves a larger constellation of actors than Ukraine, and our dyadic analysis may overlook significant interactions elsewhere, particularly between actors with more developed cyber capabilities (e.g. Russia, U.S.). We also lack interview evidence that might help contextualize the null effect. However tentative, these results do align with what we saw in Ukraine: low-level cyber attacks have had little or no impact on violence.

Conclusion

The evidence we presented in this paper – based on analysis of new data and expert interviews – suggests that cyber attacks are ineffective as a tool of coercion in war. Although kinetic operations explain the timing of other kinetic operations, low-level cyber attacks have no discernible effect on violence in the physical world. In Ukraine and Syria, the "cyberwar" has unfolded in isolation from the rest of the conflict.

This finding has several implications for theory and policy. First, by providing the first statistical analysis of modern low-level cyber campaigns, our study complements the qualitative focus of previous empirical work. Second, our research sheds light on a theoretical question regarding the strength and direction of the cyber-kinetic relationship, and – in so doing – begins to fill an empirical gap in political science literature on this topic. Third, to the extent that policymakers might over-estimate the importance of cyber actions due to a lack of empirical evidence to the contrary, our findings can potentially help correct this misperception. Finally, and more worryingly, our results suggest that – because they are so disconnected from physical violence – low-level cyber attacks are very difficult to predict.

Further research is needed to understand the dynamics of low-level cyber attacks. Our scope in this paper has been exclusively on short-term military consequences, rather than long-term political effects. The latter are no less theoretically significant, but – unlike simple counts of violent

events – potentially more difficult to measure and analyze. A study of long-term political effects would also need to more systematically incorporate purely propagandistic cyber activities and their impact on public opinion, which we omitted here due our focus on short-term military compellence.

Although the secretive nature of many ongoing physical and digital operations is a challenge for this research, questions over the coercive potential of cyber attacks will become only more salient in the future. In June 2017, the *New York Times* reported that U.S. cyber efforts against the Islamic State – previously lauded as "a [major] shift in America's war-fighting strategy and power projection" (Sabah 2016) – have yielded few tangible successes (Sanger and Schmitt, 2017). Our data from Ukraine indicates that the U.S. experience may be part of a broader pattern.

At best, coordination between low-level cyber and kinetic operations today is on roughly the same level as that between air power and ground operations in World War I. Back then, armies were increasingly using aircraft for reconnaissance and surveillance on the front, but were not yet able to fully exploit their potential for ground combat support and strategic bombing. That revolution appeared on the battlefield twenty five years later, with devastating effect. As cyber capabilities develop and synchronization challenges become less severe, there will be a growing need for assessments of how far we have come. We hope that analyses of the sort we provided in these pages can serve as an early benchmark.

References

Andres, Richard. 2012. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." *Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. 1st ed. Washington DC: Georgetown University Press* .

Andress, Jason and Steve Winterfeld. 2013. *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Atran, Scott. 2003. "Genesis of suicide terrorism." *Science* 299(5612):1534–1539.

Axelrod, Robert. 2014. "A Repertory of Cyber Analogies." *Cyber Analogies* .

Axelrod, Robert and Rumen Iliev. 2014. "Timing of cyber conflict." *Proceedings of the National Academy of Sciences* 111(4):1298–1303.

Bailard, Catie Snow. 2015. "Ethnic conflict goes mobile Mobile technology?s effect on the opportunities and motivations for violent collective action." *Journal of Peace Research* .

Baum, Matthew A and Yuri M Zhukov. 2015. "Filtering revolution: Reporting bias in international newspaper coverage of the libyan civil war." *Journal of Peace Research* 9:10–11.

Bejan, Vladimir and William S Parkin. 2015. "Examining the effect of repressive and conciliatory government actions on terrorism activity in Israel." *Economics Letters* .

Cartwright, James and W James. 2010. "Joint terminology for cyberspace operations." *Joint Chiefs of Staff (JCS) Memorandum, Nov* .

Cha, Victor D. 2000. "Globalization and the study of international security." *Journal of Peace Research* 37(3):391–403.

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

Crabtree, Charles, David Darmofal and Holger L Kern. 2014. "A Spatial Analysis of the Impact of West German Television on Protest Mobilization During the East German Revolution." *Journal of Peace Research* .

CrowdStrike. 2016. Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units. Technical report CrowdStrike Global Intelligence Team.
URL: *https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf*

Czosseck, Christian and Kenneth Geers. 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Vol. 3 Ios Press.

Davenport, Christian and Allan Stam. 2006. "Rashomon goes to Rwanda: Alternative accounts of political violence and their implications for policy and analysis." *Unpublished manuscript (http://www. gvpt. umd. edu/davenport/dcawcp/paper/mar3104. pdf)* .

Enders, Walter and Todd Sandler. 2000. "Is transnational terrorism becoming more threatening? A time-series investigation." *Journal of Conflict Resolution* 44(3):307–332.

Eun, Yong-Soo and Judith Sita Aßmann. 2014. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." *International Studies Perspectives* .

Gartzke, Erik. 2013. "The myth of cyberwar: bringing war in cyberspace back down to Earth." *International Security* 38(2):41–73.

Geers, Kenneth. 2015. "Cyber war in perspective: Russian aggression against Ukraine." *Tallinn: CCDCOE* .

Gohdes, Anita R. 2014. "Pulling the Plug: Network Disruptions and Violence in Civil Conflict?".

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.

Griniaiev, Sergei. 2004. "Pole bitvy:kiberprostranstvo." *Mn: Harvest* .

Hare, Forrest. 2012. The signifi cance of attribution to cyberspace coercion: A political perspective. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. IEEE pp. 1–15.

Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*.

Il'chenko, Oleksandr. 2016. "Rozstily Oleha Kalashnikova i Olesya Buzyny - rik potomu [Shootings of Oleg Kalashnikov of Oles Buzina - a year later]." *Segodnya* .

Interviews. 2015. "Cyber and information warfare in Ukraine.".

Junio, Timothy J. 2013. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36(1):125–133.

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

Kissel, Richard. 2013. "Glossary of Key Information Security Terms.".

Lemay, Antoine, José M Fernandeza and Scott Knight. 2010. Pinprick attacks, a lesser included case. In *Conference on Cyber Conflict Proceedings*. pp. 183–194.

Libicki, M. 2015. The Cyberwar that Wasn't. In *Cyber War in Perspective: Russian aggression against Ukraine*, ed. Kenneth Geers. NATO Cyber Center of Excellence.

Libicki, Martin C. 2007. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press.

Libicki, Martin C. 2009. *Cyberdeterrence and cyberwar*. Rand Corporation.

Libicki, Martin C. 2011. "Cyberwar as a confidence game." *Strategic Studies Quarterly* 5.

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.

Lynn, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* pp. 97–108.

Martin-Shields, Charles Patrick. 2013. "Inter-ethnic Cooperation Revisited: Why mobile phones can help prevent discrete events of violence, using the Kenyan case study." *Stability: International Journal of Security and Development* 2(3):Art–58.

Maurer, Tim and Kenneth Geers. 2015. "Cyber Proxies and the Crisis in Ukraine." *NATO CCD COE Publications* .

McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36(1):109–119.

Nye Jr, Joseph S. 2010. Cyber power. Technical report DTIC Document.

Ottis, Rain. 2010. From Pitch Forks to Laptops: Volunteers in Cyber Conflicts. In *Conference on Cyber Conflict. Proceedings*. pp. 97–109.

Pape, Robert A. 2003. "The strategic logic of suicide terrorism." *American political science review* 97(03):343–361.

Pape, Robert A. 2014. *Bombing to win: Air power and coercion in war*. Cornell University Press.

Pevehouse, Jon C and Joshua S Goldstein. 1999. "Serbian compliance or defiance in Kosovo? Statistical analysis and real-time predictions." *Journal of Conflict Resolution* pp. 538–546.

Pierskalla, Jan H and Florian M Hollenbach. 2013. "Technology and collective action: The effect of cell phone coverage on political violence in Africa." *American Political Science Review* 107(02):207–224.

Rid, Thomas. 2012. "Cyber war will not take place." *Journal of Strategic Studies* 35(1):5–32.

Rios, Billy K. 2009. "Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack." *The Virtual Battlefield: Perspectives on Cyber Warfare* 3:143.

Sabah, Daily. 2016. "Cyber bombs being used to destroy Daesh: US defense chief.".

Sanger, David. 2016. "U.S. Cyberattacks Target ISIS in a New Line of Combat." *The New York Times* .

Sanger, David E. and Eric Schmitt. 2017. "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS." *New York Times* p. A5.
URL: *https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html*

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

Schmitt, Michael N. 1999. "Computer network attack and the use of force in international law: thoughts on a normative framework." *Columbia Journal of Transnational Law* 37:1998–99.

Sharma, Amit. 2010. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34(1):62–73.

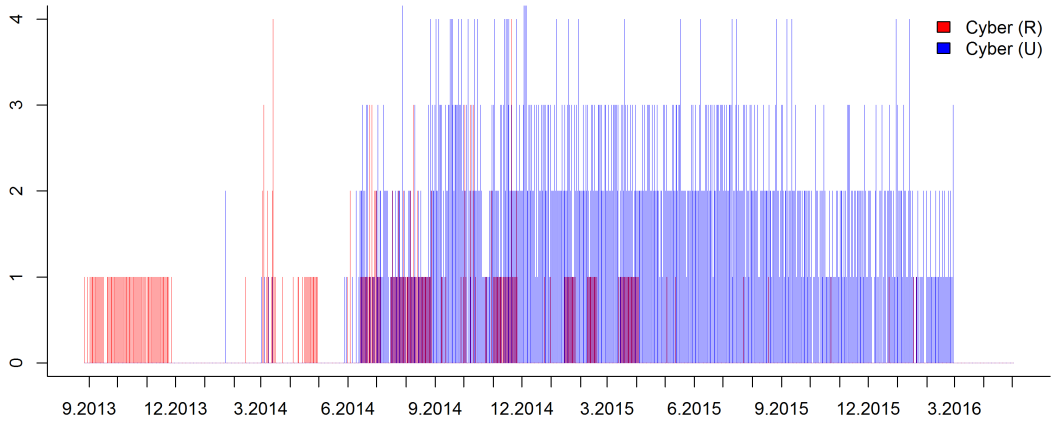
Valeriano, Brandon and Ryan C Maness. 2014. "The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research* 51(3):347–360.

Weidmann, Nils B. 2015. "Communication, technology, and political conflict Introduction to the special issue." *Journal of Peace Research* 52(3):263–268.

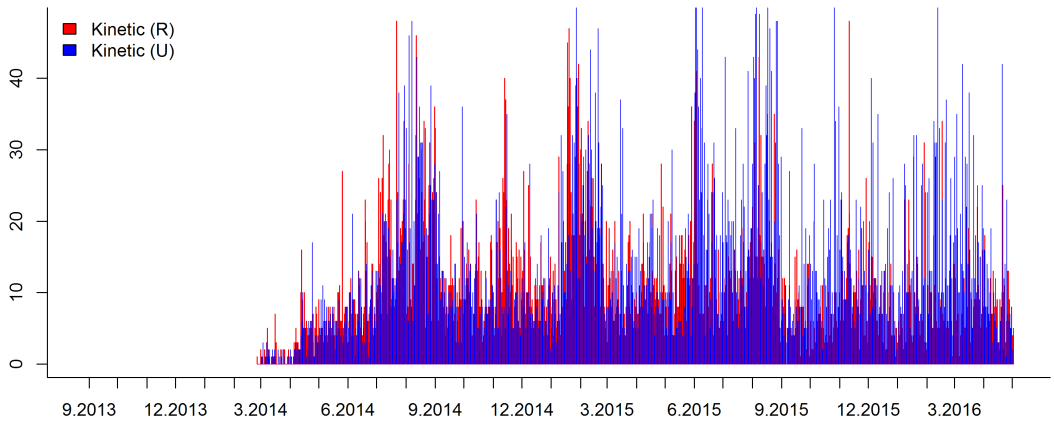
Woolley, John T. 2000. "Using media-based data in studies of politics." *American Journal of Political Science* pp. 156–173.

Zetter, Kim. 2017. "The Ukrainian Power Grid Was Hacked Again." *Motherboard* .
URL: *http://bit.ly/2jEUqW3*

Figure 1: CYBER AND KINETIC OPERATIONS IN UKRAINE (March 2014 - February 2016). U (blue) indicates operations by Ukrainian government forces; R (red) indicates operations by pro-Russian rebel groups.



(a) Cyber



(b) Kinetic

Table 1: Actors and Targets (Ukraine & Syria)

Ukraine					
Pro-Kyiv	Actor/Target	*Frequency (%)*	*Pro-rebel*	Actor/Target	*Frequency (%)*
Anonymous Ukraine	A	6 (<1)	Cyber Berkut	A	134(7)
Ukrainian Cyber Forces	A	1392(76)	Cyber Riot Novorossiya	A	41(2)
Ukrainian governmental units and officials	A/T	3(<1)/326(18)	Green Dragon	A	1(<1)
Ukrainian army units	T	1(<1)	Quedagh	A	1(<1)
Western governments and organizations	T	15(1)	Crimean government officials	T	6(<1)
Western non-state actors	T	7(<1)	Russian army units	A/T	1(<1)/14(1)
Non-state supporters	T	91(5)	Non-state supporters	T	444(24)
			Rebel groups	A/T	2(<1)/926(50)
			Russian state units and government officials	A/T	2(<1)/14(1)
			Russian state-sponsored groups	A	237(13)
Total		*1841(100)*			*1841(100)*
Syria					
Anti-Assad	Actor/Target	*Frequency (%)*	*Pro-Assad*	*Frequency (%)*	Actor/Target
Anonymous/Anonymous-sponsored units	A	93(14)	ISIL/ISIL-sponsored units	A	54(8)
Anti-Assad non-state actors	A/T	297(44)/18(3)	Russian government units	A	3(< 1)
Jabhat al-Nusra-sponsored units	A	1(< 1)	Syrian government units and officials	A/T	2(<1)/272(40)
Kurdish non-state opposition	A	11(< 2)	Syrian state-sponsored units	A/T	102(15)/2(<1)
Free Syrian Army	T	1(< 1)	Pro-Assad non-state actors	T	179(26)
Pro-ISIL social media and websites	T	140 (21)			
Total		*682(100)*			*682(100)*

Table 2: Types of cyber operations (Ukraine and Syria)

Propaganda	*Ukraine (%)*	*Syria (%)*	*Disruption*	*Ukraine (%)*	*Syria (%)*	*Both*	*Ukraine (%)*	*Syria (%)*
PPI - publishing online private information of the members of the conflicting parties	47(2)	59(9)	**AVG** - audio-, video-, and geo-intelligence collection	423(23)	1(<1)	**WDT** - website defacement	51(3)	389(57)
PRM/PUM- posting pro-rebel and pro-Ukrainian messages online	54(3)/5(<1)	——	**CPI** - collecting private information via open sources	13(<1)	10(<2)			
UWP - updating online pages	6(<1)	——	**DDS** - distributed denial-of-dervice attack	499(27)	78(11)			
			ODS - other attacks with a purpose of disruption or espionage	9(1)	10(<2)			
			SPE - spear-phishing email	234(13)	17(2.5)			
			STM - sending massive text messages or calling phones nonstop	40(2)	1(<1)			
			WBG - website blockage	257(14)	376(55)			
			WFC - gaining control of Wi-Fi access points and changing them to those of the opponent's	31(<2)	——			
Total	1841(100)	682(100)		1841(100)	682(100)		1841(100)	682(100)

Figure 2: Impulse-response matrix, daily time series (Ukraine). Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. 'U' indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and 'R' indicates operations by pro-Russian rebel forces.

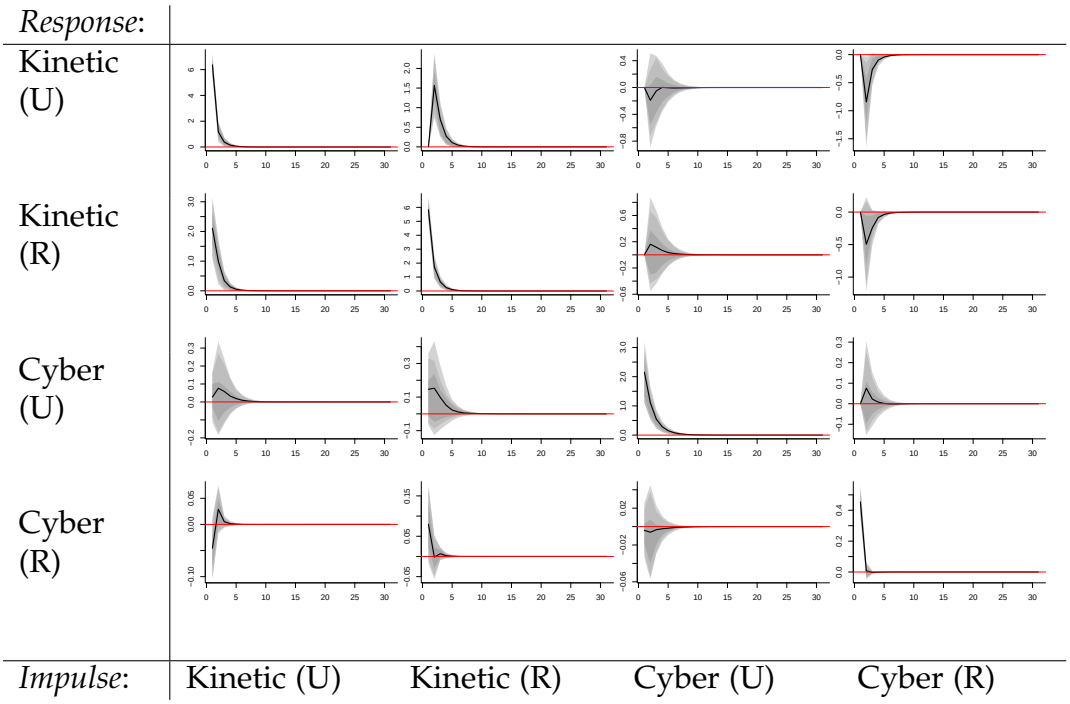


Table 3: Granger causality test, daily time series (Ukraine). 'U' indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and 'R' indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	40.26	0.00
Cyber (U) → Kinetic (U)	0.50	0.48
Cyber (R) → Kinetic (U)	0.09	0.76
Kinetic (U) → Kinetic (R)	12.29	0.00
Cyber (U) → Kinetic (R)	1.44	0.23
Cyber (R) → Kinetic (R)	2.70	0.10
Kinetic (U) → Cyber (U)	1.40	0.24
Kinetic (R) → Cyber (U)	1.88	0.17
Cyber (R) → Cyber (U)	0.00	0.95
Kinetic (U) → Cyber (R)	1.74	0.19
Kinetic (R) → Cyber (R)	0.14	0.71
Cyber (U) → Cyber (R)	0.89	0.35

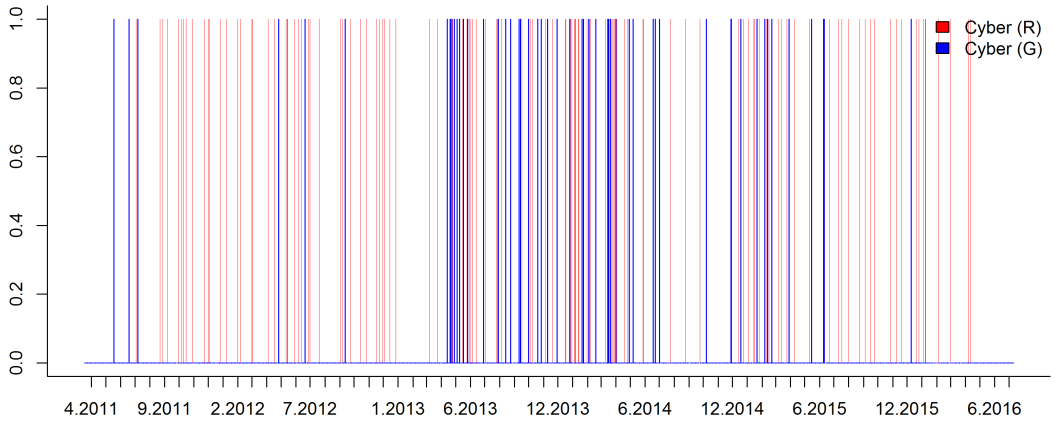
Table 4: VARIANCE DECOMPOSITION, DAILY TIME SERIES (UKRAINE). 'U' indicates kinetic and cyber operations by pro-Ukrainian government forces, and 'R' indicates operations by pro-Russian rebel forces.

	Kinetic (U)	Kinetic (R)	Cyber (U)	Cyber (R)
Kinetic (U)				
1 day	1.000	0.000	0.000	0.000
2 days	0.920	0.060	0.002	0.018
7 days	0.906	0.071	0.002	0.020
30 days	0.906	0.071	0.002	0.020
Kinetic (R)				
1 day	0.108	0.892	0.000	0.000
2 days	0.121	0.873	0.000	0.006
7 days	0.122	0.870	0.000	0.008
30 days	0.122	0.870	0.000	0.008
Cyber (U)				
1 day	0.000	0.002	0.998	0.000
2 days	0.000	0.002	0.997	0.000
7 days	0.000	0.003	0.997	0.000
30 days	0.000	0.003	0.997	0.000
Cyber (R)				
1 day	0.012	0.023	0.000	0.964
2 days	0.014	0.023	0.001	0.962
7 days	0.015	0.023	0.001	0.961
30 days	0.015	0.023	0.001	0.961

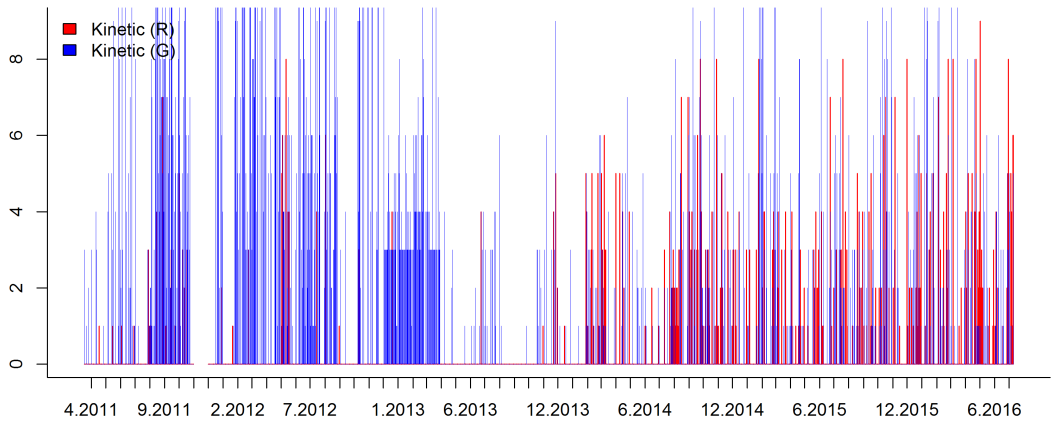
Table 5: Robustness checks (Ukraine and Syria)

Ukraine (Main results) (5/11/14-2/15/15)							
ID	*Cyber*	*IRF(d)*	*IRF(w)*	*IRF(o)(d)*	*IRF(o)(w)*	*IRF(d) Sources (RU)*	*IRF(d) Sources (U)*
1	Disruption & both	Kin(R)↔Kin(U)	Kin(U)→Kin(R)	Kin(R)↔Kin(U)	Kin(U)↔Kin(R)	Kin(U)↔Kin(R)	Kin(U)→Kin(G)
ID	*Cyber*	*GCT (w)*	*VD (d)* (30-day)	*VD(w)* (12-week)			
1	Disruption & both		Kin(R)→7%Kin(U) Kin(R)→2%Cyb(R) Kin(U)→12%Kin(R) Kin(U)→2%Cyb(R)	Kin(R)→10%Cyb(R) Kin(U)→21%Kin(R) Kin(U)→17%Cyb(R) Cyb(U)→4%Cyb(R)			
Ukraine (3/22/14-2/29/16)							
ID	*Cyber*	*IRF(d)*	*IRF(w)*	*GCT (d)*	*GCT (w)*	*VD (d)* (30-day)	*VD(w)* (12-week)
2	All	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)↔Kin(U) Cyb(U/R)↔Kin(U) Cyb(U)↔Kin(R)	Kin(R)→Kin/Cyb(U) Kin(U)→Cyb(R)	Kin(R)→3%Kin(U) Kin(U)→17%Kin(R)	Kin(R)→8%Kin(U) Kin(U)→45%Kin(R) Kin(U)→3%Cyb(R)
3	Propaganda	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)→Kin(U) Kin(U)→Kin(R) Cyb(U)→Kin(U)	Kin(R)↔Kin(U) Cyb(U)→Kin/Cyb(R) Kin(U)→Cyb(R)	Kin(R)→Kin(U)/Cyb(R) Kin(U)→Cyb(R)	Kin(R)→3%Kin(U) Kin(U)→18%Kin(R)	Kin(R)→9%Kin(U) Kin(R)→3%Cyb(R) Kin(U)→46%Kin(R) Kin(U)→5%Cyb(U) Kin(U)→2%Cyb(R)
4	Disruption	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)↔Kin(U) Cyb(U)↔Kin(U/R)	Kin(R)→Kin/Cyb(U)	Kin(R)→3%Kin(U) Kin(U)→17%Kin(R)	Kin(R)→8%Kin(U) Kin(U)→45%Kin(R)
5	Disruption & both	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)↔Kin(U) Cyb(U)↔Kin(R) Kin(U)→Cyb(U)	Kin(R)→Kin/Cyb(U) Kin(U)→Cyb(R)	Kin(R)→3%Kin(U) Kin(U)→17%Kin(R)	Kin(R)→8%Kin(U) Kin(U)→45%Kin(R)
Ukraine (5/11/14-2/11/15)							
6	All	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(U)→Kin(R)	Kin(R)↔Kin(U)		Kin(R)→7%Kin(U) Kin(U)→13%Kin(R)	Kin(R)→2%Cyb(U) Kin(R)→18%Cyb(R) Kin(U)→30%Kin(R) Kin(U)→2%Cyb(U/R) Cyb(U)→4%Kin(R) Cyb(R)→3%Kin(U)
7	Propaganda	Kin(R)→Kin(U) Kin(U)→Kin(R)	Cyb(R)→Kin(U) Kin(U)→Kin(R)	Kin(R)↔Kin(U)	Kin(R)→Cyb(R)	Kin(R)→7%Kin(U) Kin(U)→13%Kin(R)	Kin(U)→27%Kin(R) Kin(U)→4%Cyb(U) Kin(R)→5%Cyb(U) Kin(R)→3%Cyb(R) Cyb(U)→9%Kin(U) Cyb(U)→2%Kin(R) Cyb(U)→20%Cyb(R) Cyb(R)→5%Kin(U) Cyb(R)→2%Cyb(U)
8	Disruption	Kin(R)→Kin(U) Kin(U)→Kin(R)	Kin(U)→Kin(R)	Kin(R)↔Kin(U)	Kin(U)→Cyb(U)	Kin(R)→7%Kin(U) Kin(R)→2%Cyb(R) Kin(U)→12%Kin(R) Cyb(R)→2%Kin(U)	Kin(U)→29%Kin(R) Kin(U)→34%Cyb(U) Kin(U)→22%Cyb(R) Kin(R)→3%Kin(U) Kin(R)→10%Cyb(U) Kin(R)→13%Cyb(R) Cyb(U)→2%Kin(U) Cyb(U)→6%Cyb(R) Cyb(R)→3%Kin(R) Cyb(R)→7%Cyb(U)
Syria (3/17/2011-7/10/2016)							
9	Disruption & both	Kin(G)→Kin(R)		Kin(R)↔Kin(U)		Kin(U)→2%Kin(R)	
IRF: impulse response functions; GC: Granger causality tests; VD: variance decomposition; *d*: daily; *w*: weekly; *o*: alternative orderings; *RU*: Russian; *UI*: Ukrainian							

Figure 3: CYBER AND KINETIC OPERATIONS IN SYRIA (March 2011 - July 2016). G (blue) indicates operations by pro-Assad government forces; R (red) indicates operations by anti-Assad rebel groups.



(a) Cyber



(b) Kinetic

Figure 4: Impulse-response matrix, daily time series (Syria). Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. 'G' indicates reported kinetic and cyber operations by pro-Assad government forces, and 'R' indicates operations by anti-Assad rebel forces.