Information and Communication Technologies, Wartime Informing, and Insurgent Violence[*]

Andrew Shaver[†]

HiCN Working Paper 215

April 2016

Abstract:

In this piece, I explore the relationship between wartime informing by civilians, information and communication technologies, and the production of violence by insurgents. Using newly declassified data on calls - both false and legitimate - placed to a "tips" telephone hotline operated by British forces in Iraq's Basra region during the recent Iraq war, I show that while insurgents' efforts to overwhelm the platform were extensive - on some days, roughly 1200 false calls were received for every five legitimate tips provided by informants - intelligence received through the line appears to have led to reductions in particular types of wartime violence. This piece makes two fundamental contributions to the security studies literature: first, it provides evidence that while ICT platforms may tend to favor the efforts of non-state actors to mobilize against more powerful state targets, once conflict is initiated, such technologies can benefit the state by upsetting the information asymmetry upon which rebels often rely. Second, and more fundamentally, the piece offers the first direct quantitative evidence using actual "tips" data of the centuries-old proposition that information plays a central role during insurgency contests.

Introduction

The relationship between sub-state conflict and information and communication technologies (ICT) is the focus of much recent scholarly work [Pierskalla and Hollenbach, 2013, Shapiro and Weidmann, 2015, Howard et al., 2011, Manacorda and Tesei, 2016, Shapiro and Siegel, 2015, Steinert-Threlkeld, 2016, Dafoe and Lyall, 2015, Weidmann, 2015]. As Dafoe & Lyall [2015, p. 401] observe, "[w]e appear... to be standing at the threshold of an ICT-driven transformation of [poltical conflict] that will rival the introduction of earlier technologies such as the telegraph, newspaper, radio, and television."

Researchers have focused primarily on ICT's role in facilitating the mobilization of violent political actors. For instance, Pierskalla & Hollenbach [2013, p. 220] consider the spread of cellular telephones in Africa, which they find has increased conflict likelihood on that continent by providing a path for collective action: the technology "boost[s] rebels['] [capacity] to communicate and monitor ingroup behavior, thus increasing in-group cooperation. [It also] allow[s] for coordination of insurgent activity across geographically distant locations." In a similar study that instruments for cellular telephone coverage with lightening strikes, Manacorda & Tesei [2016, p. 1] find that over the past decade, across the African continent, "mobile phones [have been] instrumental to mass mobilization during economic downturns, when reasons for grievance emerge and the cost of participation falls."

Much less is known about the ways in which information and communication technologies affect conflict processes once underway. Shapiro & Weidmann (2015) find the spread of ICT during the recent Iraq war was associated with reductions in insurgent violence perpetrated against Coalition and state forces. Thus, whereas ICT appears on balance to favor relative weak sub-state actors seeking to mobilize against a state, in the Iraq case, once conflict was initiated, available ICT appears to to have favored the state. Yet, the mechanism(s) of action responsible for reductions in the intensity of ongoing conflict are not fully established theoretically or empirically. Shapiro & Weidmann hypothesize that the diffusion of ICT may reduce insurgent violence through two non-exclusive mechanisms. Such technologies may provide civilians the means of discreetly supplying information to counterinsurgents (for instance, by allowing them to call an anonymous "tips"

hotline). Insurgents' use of ICT might also create "opportunities for signals intelligence collection" [Shapiro and Weidmann, 2015, p. 249].

In this study, I explore the relationship between ICT, wartime informing by civilians, and the effects of informing through ICT channels on the production of violence by insurgents. I begin by analyzing ICT-based tipping platforms and their potential vulnerabilities to insurgent exploitation. I then use newly declassified data on calls placed to a "tips" telephone hotline operated by British forces in Iraq's Basra region during the recent Iraq war to assess its efficacy as a counterinsurgency tool. I supplement the quantitative analysis that uses the tips hotline data with qualitative analysis based a series of wartime documents, many of which were recently declassified for me for the purposes of this and related studies, by the U.S. and British governments, as well as with insights gleaned through a series of interviews that I conducted with present and former U.S. and Iraqi government employees involved in some capacity with the "tips" hotlines that operated during the Iraq war.

The results of the analysis are consistent with findings by Shapiro & Weidmann (2015). Despite considerable efforts by insurgents to overwhelm ICT tipping platforms, their existence appears to have reduced insurgent violence in southern Iraq by providing civilians with the means to supply information on insurgents. In particular, citizen tips appear to have led British forces to both unexploded roadside bombs, which they then cleared, as well as to weapons caches.

The Role of Information in Insurgency

Counterinsurgency theorists and practitioners alike have long held that information is central to the outcome of insurgency contests [Galula, 2006, Lyall et al., 2015, Berman et al., 2011, Lyall and Wilson, 2009, Shaver and Shapiro, 2016, Leites and Wolf Jr, 1970, Shapiro and Siegel, 2015]. While state forces are often militarily superior to the insurgents they fight, the former often lack information about the insurgency – the identities of its members, the locations of its safe houses and weapons caches, "how [it] operates, when it is likely to attack, in units of what size..." [Leites and Wolf Jr, 1970, p. 136]. Thus, although a power asymmetry tends to favor counterinsurgents, such advantage is offset to a greater or lesser extent by an information asymmetry that favors

insurgents. Kalyvas [2006, p. 89] describes this dynamic at work during the Soviet occupation of Afghanistan, where better equipped "Soviet soldiers... referred to their Afghan adversaries as *dukhi*, the Russian word for ghosts... and summarized the problem they faced as follows: 'You see me, but I don't see you."'

As Galula [2006, p. 50] observed more than five decades ago, "[i]ntelligence is the principal source of information on guerrillas, and intelligence has to come from the population..." Thus, citizens' decision to provide or withhold information is, therefore, thought to play a central role in insurgency contests. Although the number of citizens with substantial knowledge about an insurgency in any given conflict may be limited, citizens' collective observations can be pooled to paint a comprehensive picture of an insurgency and its operations. For this reason, Berman et al. [2011, p. 773] argue that "the silence of the population, or a substantial portion thereof, is critical for insurgent success." Civilian informers threaten to erode the informational barriers that limit counterinsurgents' ability to engage insurgents in direct military confrontations, and this dynamic renders information "a central resource in civil wars: counter-insurgents seek it, insurgents safeguard it, and civilians often trade it" [Lyall et al., 2015, p. 833].

The recent Iraq and Afghanistan wars illustrate that information asymmetries can offset even the greatest power imbalance between opposing combatants. In those conflicts, the world's military superpower led a coalition of allied nations in a fight against native insurgents and foreign fighters who had access to little more than small arms, low quality mortars, and improvised explosive devices.[1] Despite the overwhelming power imbalance, insurgents in both countries persisted in carrying out hundreds of thousands of attacks against coalition forces in the near decade-long conflict in Iraq and for even longer in Afghanistan.

---

[1]The complete sets of data on insurgent attacks carried out against Coalition forces during the Iraq and Afghanistan war as recorded by the U.S. military, which were recently released to the author, show that insurgents carried out direct fire attacks (those typically involving small arms) more frequently than any other type.

ICT, Information Flow, and Battlefield Outcomes

ICT Tipping Platforms in Recent History

With the development and diffusion of information and communication technologies, embattled governments have produced a number of platforms to facilitate the flow of information from the public. One of the earliest examples of the use of such technologies comes from the Irish Troubles. During that conflict, the Royal Ulster Constabulary established and advertised landline telephone numbers that Northern Irish citizens could call to inform on the activities of the Irish National Liberation Army and other militant organizations [Acheson, 1996].

A number of countries have since followed suit. Following the spread of the Islamic State of Iraq and the Sham (ISIS) into Iraq, that country's government reestablished tips hotlines originally established in cooperation with American and British forces that residents of affected areas of the country could use to report on the terrorist organization [Shaver and Shapiro, 2016]. Meanwhile, as Iraq's central government worked to reestablish a supply of information from the public, ISIS, in a reported effort to stop "local residents [from] phoning in tips that [are] used by U.S. and Iraqi commanders to select airstrike targets", suspended cellular telephone service in the city of Mosul [Prothero and George, 2014].

In the Philippines, which has been afflicted for decades by insurgent and terrorist violence, the National Bureau of Investigation established in 2010 a terrorism hotline to collect "tips from concerned citizens so we can respond to any incident quickly" [GMA News Online, 2010]. During the recent period of revolutionary unrest in Egypt, that country's government established a series of hotlines through which citizens could report members of the Muslim Brotherhood and terrorist organizations[2]. Pakistan's central government also recently established a series of lines that citizens can call to report "suspicious activity about terrorism" [Pakistan Hotline, 2014]. More recently, Turkey's central government, which, for years, has been locked in violent conflict with Kurdish separatists and was recently targeted in terrorist attacks carried out by ISIS has established an emergency hotline to collect information on "the identity or the location of a 'terrorist'; a plot by

---

[2]At the time of this writing, the advertisement remains live on the Egyptian Government's official police Facebook page: https://www.facebook.com/Egyptian.Police0

terrorist groups or locations of ammunition" [Daily Sabah, 2015]. Advertisements for several of these programs are displayed in Figures 1 through 3.[3]

أرقام جهاز الأمن الوطنى
للإبلاغ عن الإخوان و الإرهابيين
٢٢٦٤٥٠٠٠
٢٢٦٤٦٠٠٠
٢٢٦٤٧٠٠٠
و من خارج القاهرة أضف قبل الرقم
٠٢

Figure 1: A message advertised by Egypt's national police during the period of recent revolutionary unrest in that country: "Numbers of the national security apparatus for informing on the Muslim Brotherhood or terrorists: 22645000, 22646000, 22647000. And from outside of Cairo, first dial 02." (Author's translation.)

---

[3]Countries' use of ICT platforms for national security purposes has not been limited to counterinsurgency. For instance, to reduce the number (or freedom of operation) of foreign spies operating within its territory, China recently established a "spy hotline" for "[c]itizens concerned that they have encountered a spy'... to report [the] potential snooper" [Macauley, 2015]. Seeking assistance in locating high ranking drug cartel officials, the United States' Drug Enforcement Agency has established and advertised anonymous hotlines along the country's border with Mexico to solicit information from Mexican citizens [Epstein, 2016]. In efforts to track nationals who have travelled to Syria to fight in that country's ongoing civil war, the French and Russian governments have both established independent telephone hotlines. In France, "[p]eople are encouraged to call the number if they suspect a friend or family member is considering travelling to the country or is in danger of becoming radicalised" [FRANCE 24, 2014].

Figure 2: Advertisement for Pakistan's national 1717 terrorist tips hotline

Figure 3: Advertisement of Pakistan's regional terrorist tips hotlines

Are ICT Tipping Platforms Effective Counterinsurgency Tools?

Do ICT platforms increase the flow of information to state agents during periods of civil unrest, ultimately reducing violence levels? The answer to this and related questions has largely eluded scholars for lack of available data on information flow during conflict. As Lyall et al. [2015, p. 833] have observed, "despite its essential role in civil war dynamics, the act of informing is still poorly understood, due mostly to the classified nature of informant 'tips.'"

Given the importance of information during an insurgency, insurgents often expend considerable effort to restrict its flow. As the *Handbook for Volunteers of the Irish Republican Army* [1985, p. 27] exhorts its readers: "[t]he guerrilla... must stop the flow of information to the enemy." Thus, informing is often regarded as a "potentially life-and-death [activity]..." [Lyall et al., 2015, p. 833]. As Shaver & Shapiro [2016, p. 9] claim, "if insurgents were successful in determining that an individual had informed [during the recent Iraq war]... he or she would almost certainly be tortured and killed." Anecdotes of retaliation against informants by the Taliban [Stanford University & NYU, 2012, p. 27], ISIS [Otten, 2015], Hamas [Sherwood and Balousha, 2014], the Shining Path [Simons, 1984] and various other militant organizations are all consistent with this premise.

It, therefore, conventional wisdom that citizens tend to avoid informing. Because ICT informing platforms offer citizens a discreet and potentially anonymous means of supplying information, the spread of information and communication technologies within conflict settings would seem to facilitate information flow to the state by reducing the expected costs that would-be informants face in electing to supply information.

Shapiro & Siegel [2015, p. 313] make this argument, contrasting this apparent effect of available ICT within conflict setting with its effects on rebel communications: cellular technologies have "twin effects... they make it easier for antigovernment actors to coordinate and solve collective action problems, but they can also help government forces repress activism. Mobile phones can make it safer for progovernment civilians to collaborate with security forces; further, governments around the world have varying capacities to tap mobile communications, meaning that potential activists using cell phones create new intelligence collection opportunities for government forces."

Whether or not most governments can exploit signals intelligence opportunities made possible

by rebels' use of ICT[4], Shapiro & Siegel's argument assumes that the mere existence of ICT-based tipping platforms (at least weakly) improves a counterinsurgency's position *vis-a-vis* its opponent. Though this may typically be the case, as I argue below, the relationship between these variables is indirect and complex, and the opposite outcome is feasible as well. Whether ICT tipping platforms ultimately serve counterinsurgents interests appears to depend on whether or not these forces can limit insurgents' abilities to manipulate the platforms.

To be effective, ICT-based tipping platforms must generate a flow of credible intelligence on which counterinsurgent forces may act. Often, such information is time sensitive – for instance, as relates to impending attacks – and information received is of value only if used within a sufficiently short space of time. In cases in which insurgents enjoy large levels of popular support, they might be used only rarely by members of the public. Yet, the more interesting set of cases include those in which many members of the public are willing to supply credible information through such platforms.

Even when citizens are willing to provide tips, it does not necessarily follow that the platforms automatically improve the counterinsurgent's position. At issue are the very characteristics that make the platforms attractive to potential informants – their ease of use and the presumed anonymity that they provide users – which can serve insurgents' interests as well. In particular, insurgents might supply false information through the platforms. False information may result in two general categories of outcomes. The first of these would only limit the effectiveness of tips platforms. The second is more insidious and, in the extreme, paradoxically threatens to result in losses for the counterinsurgency.

First, false information may render credible information irrelevant or may decrease counterinsurgents' response time in using credible information received. Consider, for instance, the case of a tips hotline. So long as counterinsurgents lack the technological means to identify and block insurgents from calling, insurgents (or individuals they have recruited for such purpose) might make repeated calls that tie the line up, thereby reducing the amount of credible information ultimately received by the call-center operators. Insurgent callers might also offer false information that

---

[4]Although signals intelligence is not the focus of this piece, it is not clear that most or even many governments currently fighting insurgencies possess the technical capabilities to monitor rebels' communications over cellular networks and through the internet

appears credible (for instance, indicating that an improvised explosive device has been emplaced along a particular roadway when in fact no such device actually exists) for the purposes of reducing operators' ability to distinguish between credible and non-credible tips. Importantly, this latter strategy does not depend on whether counterinsurgent forces can ultimately adjudicate between legitimate and illegitimate tips. Even if such identification is possible, unless counterinsurgents can do so within a sufficiently short period of time, the flow of false information threatens to render time-sensitive information irrelevant.

Although sophisticated governments may, in theory, overcome these problems, at least in part, with particular technological fixes, as a review of the evidence will later show, even governments with access to the world's most sophisticated technologies appear beholden to at least some of these insurgent tactics.

Second, insurgents might discreetly supply false information that lures responding counterinsurgents into ambushes or, more simply, diverts them, enabling insurgents to carry out attacks in areas consequently left relatively more susceptible. In this set of cases, if insurgents succeed in ambushing or diverting counterinsurgents with false information more frequently than counterinsurgents act on legitimate tips, it is theoretically possible for counterinsurgents' use of such platforms to leave counterinsurgents worse off (than if they had never adopted the platforms)[5]. Although it may be tempting to assume that such extreme scenario would never actually occur because counterinsurgents would sooner stop using the platforms than they would continue to use them if they were suffering more losses than gains as a result. However, with access only to incomplete information, counterinsurgent forces may not recognize such outcomes. That is, responding counterinsurgent forces may not recognize that they have been misled.

Consider the following scenarios: In the first, counterinsurgent forces come under attack as they respond to a tip they have received. In the second, insurgents carry out an attack in one area of a city while counterinsurgents carry out operations in another area of the city in response to a tip they have received. In both cases, counterinsurgents may or may not have been responding to legitimate tips. Indeed, counterinsurgent forces routinely come under attack, including when they

---

[5]Worse off in the simple sense of comparing the number of attacks launched by insurgents against counterinsurgent forces with the number of offensive operations carried out by counterinsurgent forces that were made possible given the receipt of some number of positive and false-positive tips.

are not responding to information supplied by informants. And in intense conflict settings, like the ongoing conflicts in Syria and Afghanistan, attacks may be likely to occur within a given area whether or not counterinsurgent forces are actively conducting operations elsewhere within such area. To increase the likelihood that either type of false tip is not suspected, insurgents might even supply credible tips – for instance, tips that lead responding counterinsurgents to actual weapons caches – so that attacks carried out by insurgents as a result are more likely to be viewed as incidental to the operation itself.

The following case, described during an interview by Nouman Shubbar, an Iraqi-American adviser hired by the Coalition Provisional Authority to train and lead Iraqi police forces during raids during the early months of the Iraq war, typifies the way in which the fog of war complicates efforts to identify why an insurgent attack took place. He begins by describing how he and his team of Iraqi police officers were ambushed shortly after conducting a raid following information they had received on a suspected Baathist safehouse but ends by considering the possibility that the attack may have been simple coincidence:

> *"We fell into an ambush... when we were with the Iraqi police trying to arrest ex-Baathists. We [carried out a raid on] a house in the Shula area of Baghdad. We searched the house and arrested some [ex-Baathists and] confiscated weapons... As we left, [another adviser and I] were in the [lead vehicle] of the convoy. One of our biggest concerns was avoiding friendly fire at Coalition check points... so we would go to front [of the convoy] to be able to communicate [with those forces]... as we were traveling... the middle [car] of the convoy was attacked with small arms... there was a lot of [gun] fire... Three Iraqi cops were wounded, one severely... We had to rush him to the hospital. [The attack] could have been a coincidence... I don't know how they would have known which way we would have left [the vicinity]. It would have taken a lot to lay an ambush."* Shubbar [2016].

In the following sections, I explore the relationship between wartime informing by civilians, ICT, and the production of violence by insurgents during the Iraq and Afghanistan wars. I review qualitative evidence from both conflicts before carrying out quantitative analysis using tipline call data from the recent Iraq war.

Qualitative Evidence from the Iraq and Afghanistan Wars

A review of qualitative evidence from the Iraq and Afghanistan conflicts paints a mixed picture of the effects of ICT-based tips platforms on insurgent violence. During both wars, Coalition forces and their host-nation partners established a variety of ICT-based platforms to collect information from the public on insurgent movements.

The earliest use of tips hotlines during the Iraq war centered not on collecting information on insurgents but on securing details related to the whereabouts of deposed Baathist leader Sadaam Hussein and on instances of "police or judicial corruption." (See Figures 4 and 5.)

In an interview, Bernard Kerik, a former New York City police commissioner who served as Iraq's interim Minister of Justice before the Coalition Provisional Authority transferred affairs to the Iraqi central government, explains that he came up with the initial idea for a tips hotline in consultation with a various Iraqi military officers based on his experience having run a tips hotline in New York City. The Coalition Provisional Authority "gave us a satellite phone [and the] idea was for us to put up posters [and for the calls to] be taken by the Iraqi officers... Everyone [the Iraqi military officers] refused! They were deathly afraid of someone recognizing their voices. So, no one would take the phone: 'They'll kill me and my family.'" [Kerik, 2014]. However, after finding someone willing to answer the calls, "we put up the posters all over Baghdad... Then, within about three days, we had our first call about a kidnapping" [Kerik, 2014].

Figure 4: Saddam Hussein wanted poster with hotline telephone number and e-mail Address. Source: U.S. Coalition Provisional Authority

**AS LONG AS THERE IS CORRUPTION,
THERE WILL NEVER BE JUSTICE!**

INTIMIDATION, BRIBES, ACTS OF VIOLENCE, OR SOLICITATIONS OF
ANY TYPE ARE NOT ALLOWED UNDER ANY CIRCUMSTANCES.

IF YOU HAVE KNOWLEDGE OF POLICE OR JUDICIAL CORRUPTION WITHIN
THE COURTS, PRISONS, OR JAILS, YOU OR YOUR FAMILY CAN CALL
ANONYMOUSLY. WITH YOUR HELP IRAQ CAN STOP FUTURE CORRUPTION
IN THE COURTS, PRISONS AND JAILS.

CALL & REPORT ANONYMOUSLY TODAY!

964-1-813-6666

tips@orha.centcom.mil

Sponsored by the Ministry of Justice

IN BAGHDAD 813-6666
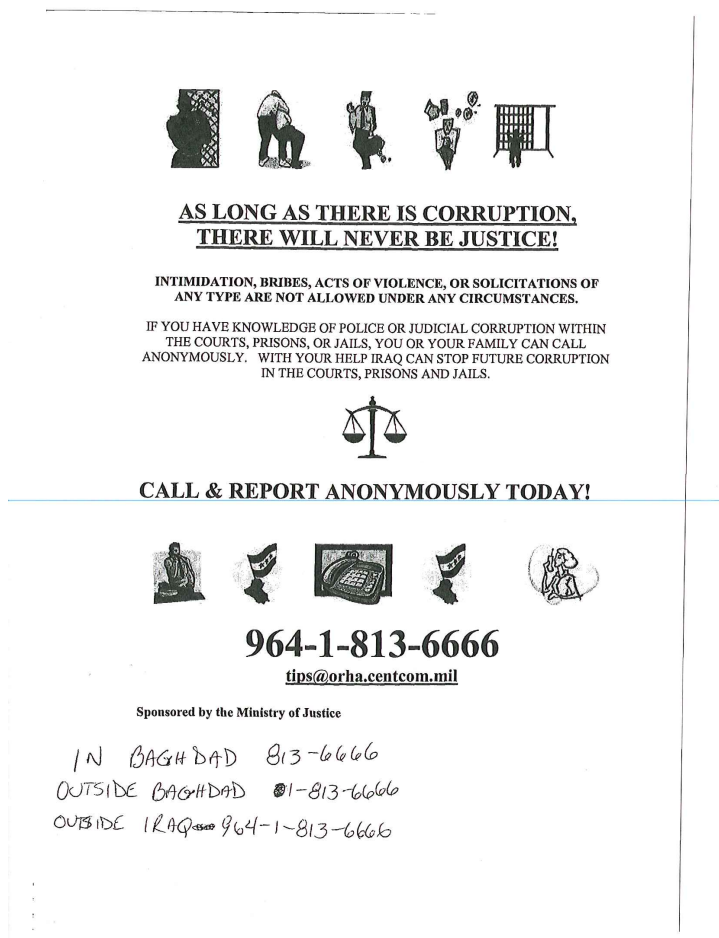OUTSIDE BAGHDAD 01-813-6666
OUTSIDE IRAQ 964-1-813-6666

Figure 5: Flyer referring individuals aware of police and judicial corruption to a tips hotline. Source: Office of the Secretary of Defense through FOIA # 15-F-0778

As the Iraqi insurgency began to intensify, American and British forces worked with Iraq's Ministry of Interior to establish the national "130 tips hotline," "an anonymous tip-off telephone hotline for reporting terrorist related activity" [U.S. Central Command, U.S. Department of Defense, 2007]. British forces operating in the country's south managed a separate regional "130" line that serviced the greater Basra area. In addition to these lines, "between 30 and 60" regional hotlines were established [U.S. Central Command, U.S. Department of Defense, 2007]. American forces established e-mail accounts with Gmail and Yahoo! (for instance, *eyesoniraq*130@*gmail.com*, *baghdadtipshotline*@*yahoo.com*, and *tipstallafar*@*yahoo.com*) to which information could be e-mailed [Task Force Baghdad PAO, 2005, BBC, 2005].

The Central Intelligence Agency developed an online Arabic-language submission platform through which "brave individuals willing to provide information leading to the arrest of terrorists

and the leaders of the extremist organizations..."[6] could supply tips.[7]

In Afghanistan, a number of regional hotlines were also established. More recently, the Afghanistan government established a national Emergency Service Call Center, to which citizens can supply information on insurgents.[8] In both countries, these platforms were advertised to Iraqi and Afghan citizens in a wide variety of ways ranging from "billboard advertisements [to] television commercials, leaflets, business cards, posters, stickers, and even cigarette lighters..." [Shaver and Shapiro, 2016, p. 13]. These are depicted in Figures 6 through 12.

Figure 6: Afghan police Ford Ranger with tip-line number on the side. Source: Small Arms Defense Journal

Figure 7: Leaflets containing tip-line numbers dropped from helicopter in Afghanistan. Source: DVIDS (U.S. Military)

---

[6]Author's translation.

[7]See: $www.cia.gov/cgi-bin/arp\_form.cgi$ and $www.cia.gov/about-cia/iraqi-rewards-program.html$

[8]They may also use the line to report corruption and to request more general emergency response services. See: http://www.eupol-afg.eu/node/244.

Figure 8: Iraqi citizen holding U.S. military issued business card containing tip-line number. Source: DVIDS (U.S. Military)

Figure 9: Soldier affixes sticker containing tip-line number in public space. Source: DVIDS (U.S. Military)

Figure 10: Posters with tip-line information in Afghanistan. Source: DVIDS (U.S. Military)

Figure 11: U.S. and Afghan soldiers distribute fliers containing tip-line information. Source: DVIDS (U.S. Military)

Figure 12: Iraqi citizen takes cigarette lighter engraved with tip-line number. Source: DVIDS (U.S. Military)

U.S. Defense Department press releases and public reports (and popular media stories based on information supplied by the Department) relating to both wars describe numerous counterinsurgency successes resulting from tips secured from local citizens. One tip, for instance, supplied "from inside Sadr City led Iraqi and coalition forces to a cache inside Sadr City of more than 450 deadly anti-tank mines" [Garamone, 2007]. Another tip is credited with leading "U.S. troops to five separate buildings near Fallujah... where they found the munitions containing chemicals, three vehicle bombs being assembled, including a truck bomb, about 65 propane tanks and 'all kinds of ordinary chemicals"' [Smith, 2007]. Yet another is described as leading to the discovery of "five

separate weapons caches west of Tarmiyah, containing a total of 41,000 pounds of explosives as well as 35 projectiles, one of the largest caches found in Salah ad Din in the last 15 months" [U.S. Department of Defense, 2007].

However, such stories are of only limited value in assessing the efficacy of the ICT platforms. First, it is unclear from these accounts whether the tips that resulted in such successes were secured through ICT platforms or through traditional channels (e.g. in-person communications). Second, the Department's strategic intentions in highlighting such stories are not fully known. For instance, for every such success story, it is unknown what number of cases occurred, if any, (but were not publicly reported) in which insurgent successfully baited Coalition or Iraqi forces by planting false tips.

A more credible body of information is contained within a series of internal documents recently released by U.S. Central Command and by the UK's Ministry of Defence. When written, these materials were not intended for public consumption. Indeed, a number of them were classified before being approved for public release, indicating that the authors expected the documents to remain sequestered when they were written. In them, government officials generally describe the national 130 tips hotline as a success. According to an internal "point paper" describing the program, "IEDs are VBIEDs [vehicle-borne improvised explosive devices] are reported and cleared, terrorists are captured, and weapons caches are seized..." [U.S. Central Command, U.S. Department of Defense, 2007]. In addition, "[t]he tips program has an excellent history of reporting both Shia and Sunni terrorist activity..." [U.S. Central Command, U.S. Department of Defense, 2007].

More specifically, this same document notes that "OCF-I [American special forces] and SCID [the Strategic Counterintelligence Directorate] describe the [130 tips hotline] program as very successful. This program provides SCID with 80% of its [human intelligence] sourcing and 100% of its operations within the past year" [U.S. Central Command, U.S. Department of Defense, 2007]. Another of these documents describes the national 130 hotline as of such great value that the U.S. President, Vice-President, and Secretary of Defense "all requested historical data for the tips program" [Multi-National Corps – Iraq, 2008].

Yet, the internal documents also describe concerted and reasonably successful efforts of insurgents to overwhelm the hotlines. As one document describes, "[t]he most pressing problem to solve is inbound call filtering / blocking of harassment and denial of service calls from insurgent groups" [Army Sustainment Command, U.S. Department of the Army, 2010]. Another document attempts to quantify the problem: "Three out of four phone calls are harassment or death threats" [U.S. Central Command, U.S. Department of Defense, 2007]. In an e-mail exchange that was included amongst the released documents, a representative of the Military Information Support Team – Iraq, the organization that managed the database of tips data received, informally describes conditions similarly: "[T]here are 15 phone lines in the call center manned by 5-6 Iraqi Police officers 24 hours a day. The phones literally ring off the hook constantly..." [U.S. Central Command, U.S. Department of Defense, 2006].

The result of these insurgent efforts was to limit the number of calls operators could answer, potentially resulting in missed information from legitimate callers: "[a]pproximately 5000 calls are received on a daily basis; this does not take into account a large number of call that hit a busy signal. Iraqi Operators are only able to answer an estimated one out of five, or roughly 1000 calls a day" [U.S. Central Command, U.S. Department of Defense, 2007].

UK Ministry of Defense documents describe similar call patterns into the regional hotline British forces managed. For instance, one document notes that for the period between July 12 and 18 of 2007, "[t]here were a total of 4774 calls to the Tips Hotline... of these calls, 2991 were malicious/nuisance calls, and 1702 were hang ups. Tips, wrong numbers or other enquiries made up the remainder" (81 calls) [UK Ministry of Defence, 2007a].

The documents also suggest that relatively few counterinsurgent responses result from tips – even amongst those with legitimate information: of the estimated 5000 calls received per day, "[a]pproximately 120 reports are drafted each day which are actionable or have some intelligence value. All reports are sent up, yet most reports do not generate a response" [U.S. Central Command, U.S. Department of Defense, 2007].

Other qualitative evidence suggests that insurgents took the tips programs quite seriously. Militants in Iraq and Afghanistan actively sought to limit their use. In Baghdad, for instance,

billboards were used to "promote the [130 national] hotline as a way for the Iraqi people to 'fight the war in secret' without fear of reprisal"; "the hotline and its success have 'hit a nerve with the insurgents' who regularly vandalize billboards promoting the campaign" [Miles, 2004].

In Afghanistan, similar observations have been made. For instance, Shapiro & Weidmann [2015, p. 248] note that "[i]n an attempt to prevent villagers from calling in tips to the military forces, [the Taliban] issued decrees ordering all cellphone towers to be turned off at night and they attacked and destroyed cellphone towers for the same purpose."

In an interview, the first tips line operator in Iraq describes having to maintain absolute secrecy about working as an operator to avoid being targeted by insurgents [tips line operator, 2014]. Similarly, Sue Coates, a former Iraqi Reconstruction Management Office employee who was associated with the central Baghdad tips hotline observes that the identities of at least some of the operators became known to the insurgents during the war [Coates, 2014]. The dangers operators faced commuting to and from the Green Zone tips call center (a small, single room trailer in the Adnan Palace area) were reportedly so great that they ultimately ended up living in the call center itself. Her account is consistent with one of the recently released Defense Department documents, which indicates that "[t]he Iraqi operators are sleeping on the floor under their desks" [U.S. Central Command, U.S. Department of Defense, 2007].

Living in such tight the quarters for an extended period of time proved to be psychologically stressful. More disturbing, however, were the continuous phone calls to which the operators had to respond. According to Ms. Coates and consistent with Defense Department reports, the center's telephones rang near incessantly and throughout the night, making it difficult for the confined operators to get any form of regular rest. By her account, in an attempt to shut the hotline down, insurgents were not only jamming the lines but terrorizing the operators.

Operator fear of insurgent retaliation also apparently complicated U.S. efforts to transition the national 130 hotline's physical location to Iraq's Ministry of Interior. Multi-National Security Transition Command – Iraq (MNSTC-I) "is working to move the Tips program to MOI-HQ in order to be co-located with the NCC. MOI-HQ is heavily infiltrated by Shia militia. Over 80% of the current Tips operators have stated clearly that they will not move to the NCC location due to

fear of death for reporting on JAM/militia activities" [U.S. Central Command, U.S. Department of Defense, 2007].

There is considerably less evidence, however, that insurgents succeeded in using the tips hotlines to ensnare counterinsurgent forces. Neither the U.S. Defense Department nor the UK Ministry of Defence documents contain any reference to efforts by insurgents to use the tips lines to either distract or ambush counterinsurgent forces with the calls they placed. I have come across only one exception. *The Times* describes a case in which a "tip led police to a booby-trapped body abandoned near a coffee shop in Baghdad, which exploded when they approached, injuring two" [Haynes, 2007].

Tips Hotline Data and Preliminary Empirical Analysis

Efforts to study wartime informing have long been limited by the highly secretive and restricted nature of information provided by civilians about an insurgency. As [Lyall et al., 2015, p. 834] have observed previously, "[t]win obstacles–the classified nature of informant data and ethical considerations in tracking such risky wartime behavior" limit scholarly inquiry. With the a single exception,[9] no quantitative analyses using direct measures of tips have been carried out by members of the academy.

In late 2015, the United Kingdom's Ministry of Defense supplied me with data on calls placed to the 130 regional hotline in addition to a series of supporting documents describing the type of tips received through such calls. British forces were responsible for Multi-National Division – South East, which comprised Iraq's Barsa, Muthanna, Dhi Qar, and Maysan provinces, and calls made within that area to the number 130 were directed to a call center run by British forces.

The call records dataset consists of the daily number of calls made to the hotline, categorized by type: a) "tips", b) "malicious"; c) "erroneous"; d) "nuisance"; and e) "other". The data cover two separate time periods, which collectively provide just under one year's worth of daily data. The first time series covers all days in the period covering June 06, 2006 through February 11,

---

[9]Shaver & Shapiro (2016) use data that Shaver secured from the U.S. Defense Department on weekly province-level data on the number of credible tips received by American forces (through both ICT and non-ICT (in-person contact, for instance) channels) for a sixty-week period of the Iraq war.

2007. The second spans all days between January 01, 2009 and February 28, 2009.

Both the MoD and U.S. Central Command records indicate that tip quality determinations were made after retrospective analysis of the outcome from each tip [UK Ministry of Defence, 2016, Multi-National Force – Iraq, 2007] For instance, tips were considered "[a]ctioned" if an "immediate on-the-ground response occured"; others were classified as "[p]ositive" if they led "to successful capture of [anti-Iraqi forces], arms or equipment, IED found and cleared, or attack prevented" [Multi-National Force – Iraq, 2007].

According to the Ministry of Defence documents, once a credible tip was received, the organization to which the information was passed would depend upon the nature of the tip itself. The large majority of tips were passed to Basra's Provincial Joint Coordination Center (PJCC) and to the Provincial Joint Operations Centres (PJOCs) serving the Muthanna, Dhi Qar, and Maysan provinces. Other organizations to which information was disseminated included (but are not limited to) the National Information and Investigation Agency (NIIA Intel), Basra's Criminal Identification Division (CID), and the Multi-National Force – Iraq Directorate of Intelligence (J2) [UK Ministry of Defence, 2007b]. In the rare instances in which a tip supplied in the Basra region regarded activity in Baghdad, information was passed to the national 130 hotline center where additional determinations on dissemination could be made.

A time series plot of legitimate tips calls received for this first period it appears in Figure 13. An average of 4.18 tips were received per day during the period. Consistent with the qualitative evidence from Iraq and Afghanistan, the data strongly support the proposition that insurgents were engaged in intensive efforts to overwhelm tips lines by tying them up. Figure 14 shows that during the first time period, erroneous, nuisance, and, in particular, malicious calls vastly exceeded tips received. This pattern can be seen even more starkly in Figure 15, in which an aggregate false calls variable – the summation of erroneous, nuisance, and, malicious calls – are plotted against tips. At their peak on October 10, 2006, 2122 false calls were received (compared with nine tips that same day). Expressed differently, over this period, the average percentage of calls received that were tips was 1.052%. A time series of this percentage expression is plotted in Figure 16.
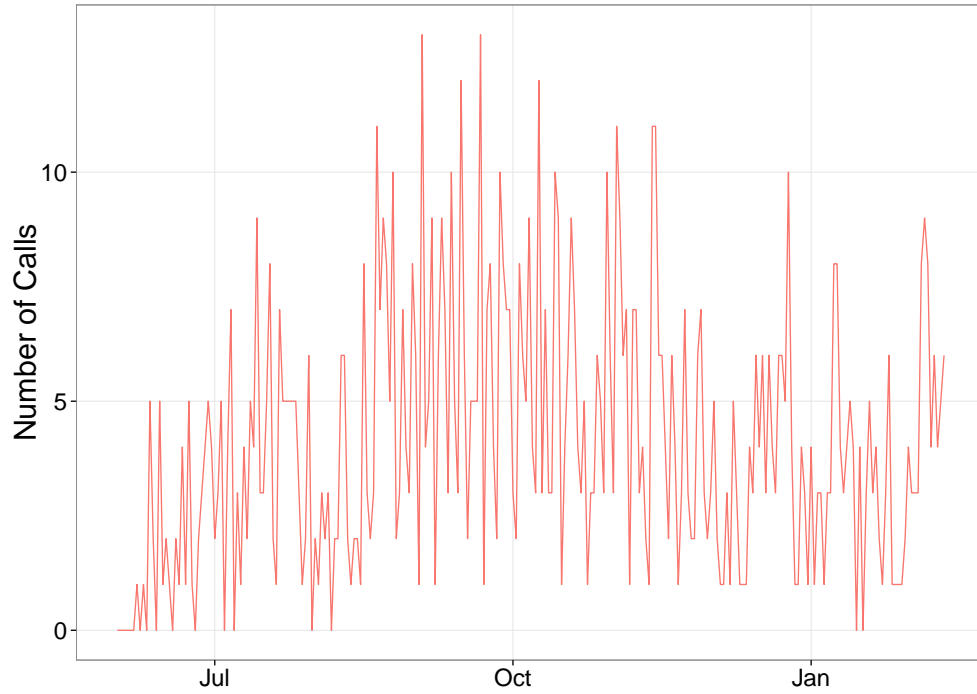
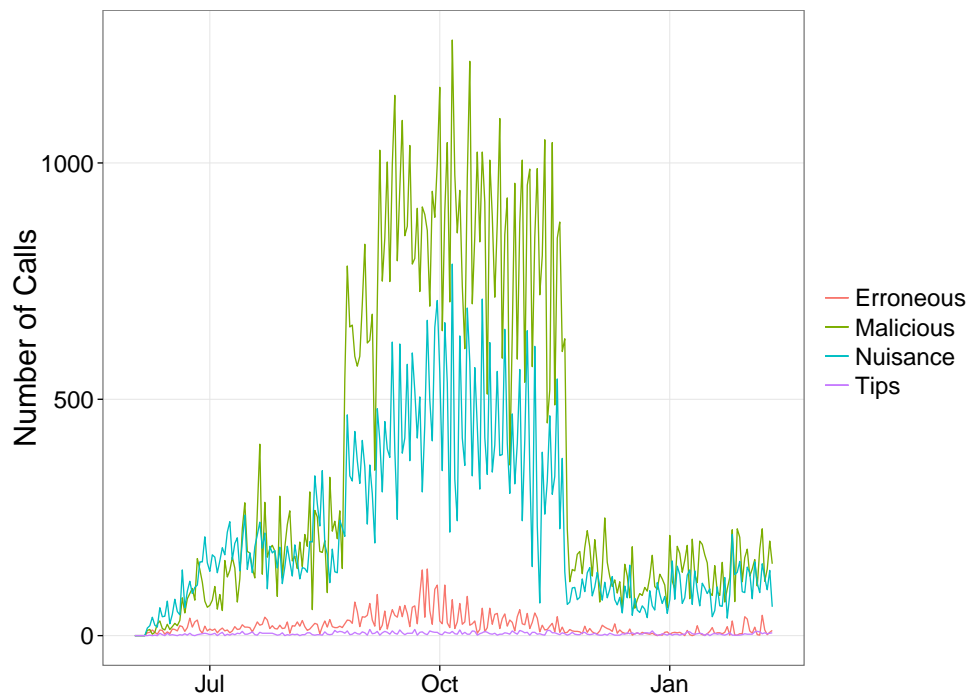Figure 13: Legitimate Tips Calls, 2006-06-06 to 2007-02-11.

Figure 14: All Calls Received by Basra-region 130 Hotline by Type, 2006-06-06 to 2007-02-11.
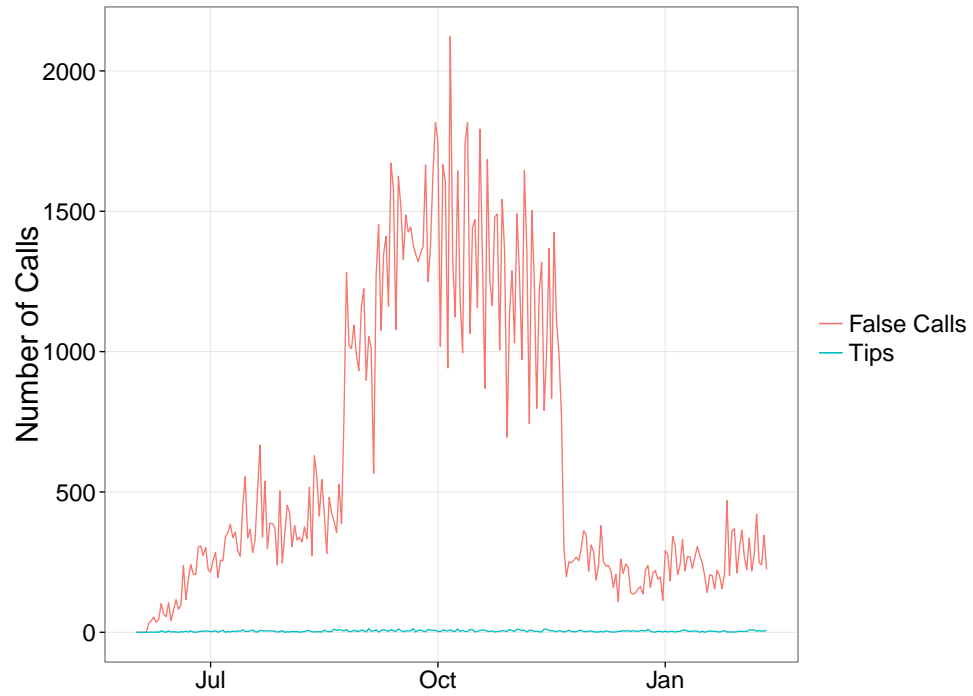
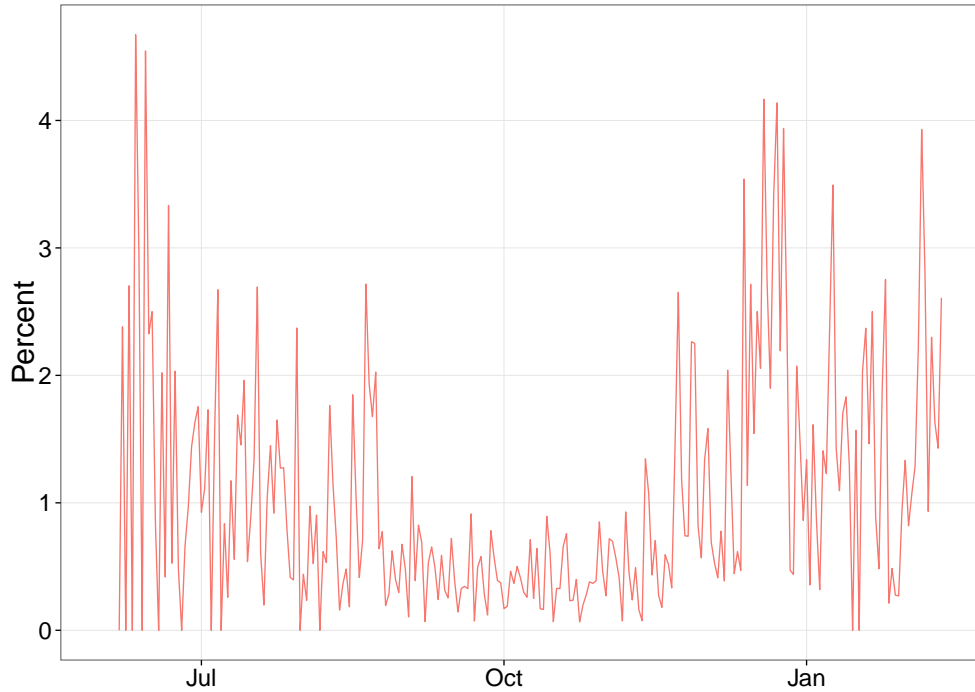Figure 15: False vs. Tips Calls Received by Basra-Region 130 Hotline by Type, 2006-06-06 to 2007-02-11.

Figure 16: Percentage of Calls Placed to Basra-region 130 Hotline that were Tips, 2006-06-06 to 2007-02-11.

A second pattern is also apparent from the data. Although false calls persistently outnumbered tips, significant changes in the number of false calls received occurred throughout the war. From the data contained in the released British document, a weekly times series covering a large range of dates can be constructed. Additional such fluctuations are apparent in this time series and can be seen in Figure 17.
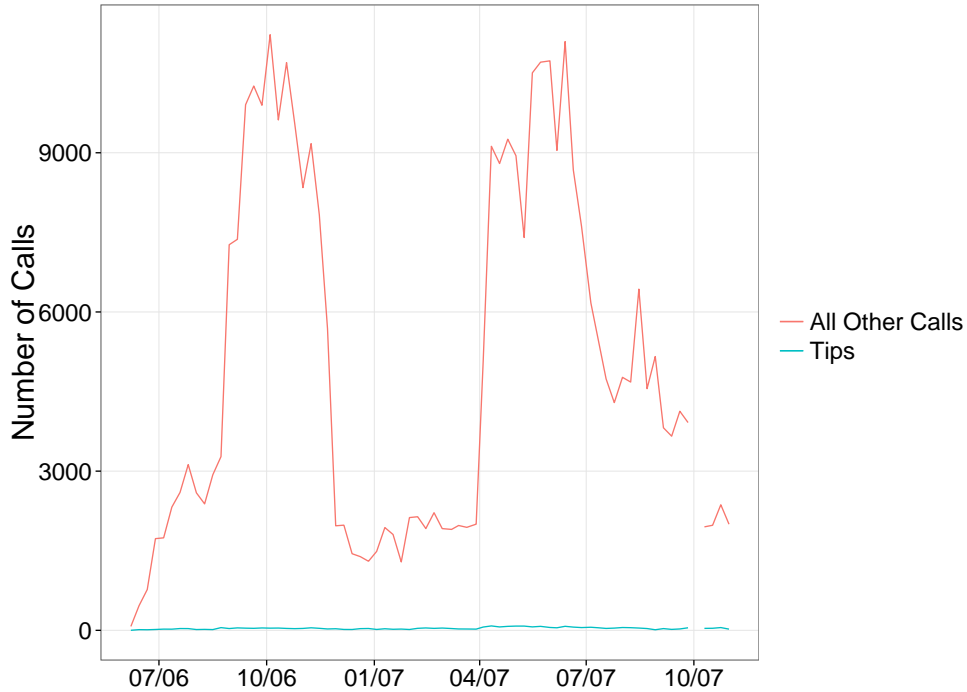
Figure 17: All Calls Received by Basra-region 130 Hotline by Week, 2006-06-06 to 2007-10-31.

In 2009, the pattern is changed. Although significantly fewer legitimate calls were received during this period (0.73 per day on average), the number of malicious, erroneous, and nuisance calls had dropped even further. In effect, the gap between the two classes of calls was greatly reduced relative to the 2006-07 period. (See Figure 18.) It is possible that by this point, British forces had developed the technical capabilities to limit the volume of spurious calls. Yet, this explanation does not account for the concurrent drop in legitimate calls. Another possibility is that there were fewer calls of all types because the insurgency had, by this point in the war period, largely died out in this region. This explanation is consistent with a plot of violent insurgent attacks in the Basra region (Figure 19), which shows that by this second period, insurgent attacks had reached their lowest levels in the conflict to date (approximately 2.63 attacks per day relative to an overall conflict average of approximately 16.84 attacks per day).
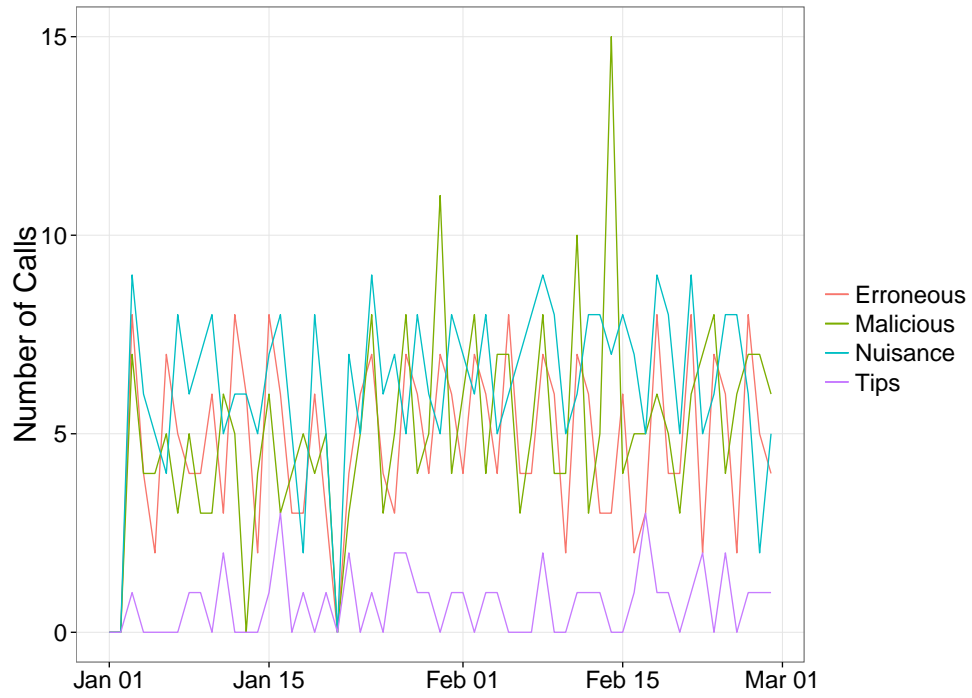
Figure 18: All Calls Received by Basra-region 130 Hotline, 2009-01-01 to 2009-02-28.
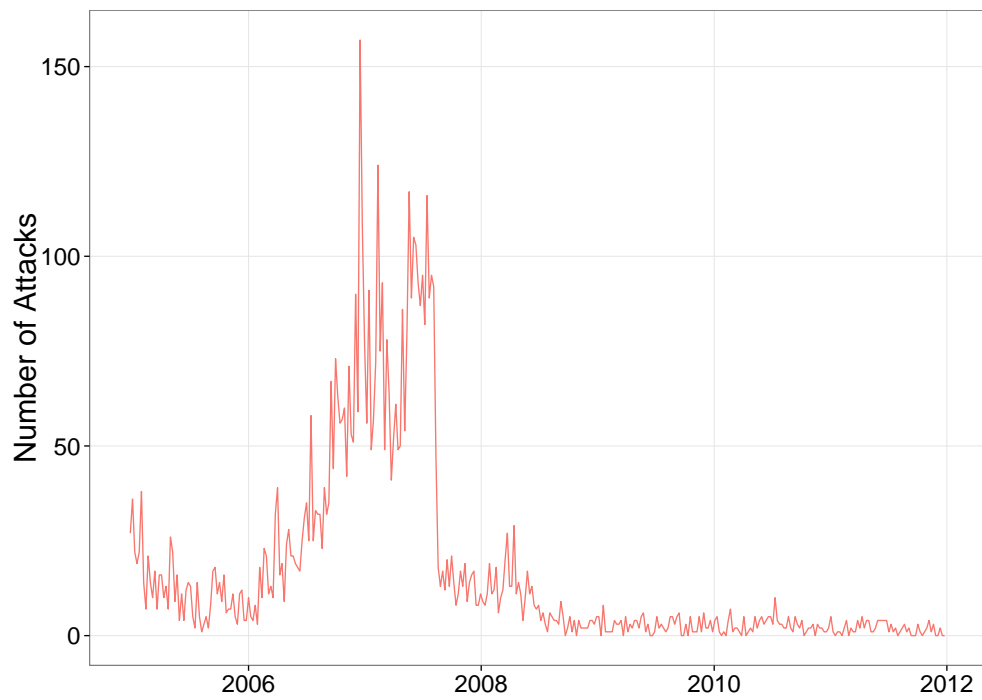

Figure 19: All Insurgent Attacks in Basra, 2005-01-01 to 2011-12-31.

In the following empirical analysis, I supplement these call records with data on insurgent and counterinsurgent activity from the Iraq war. Data on insurgent attacks by type (e.g., direct fire, indirect fire, improvised explosive device) come from the full set of Iraq war significant activities (SIGACTS) data prepared and introduced by Shaver and Tenorio [2015]. A separate dataset on all Iraq war weapons cache discoveries, also prepared and released by Shaver and Tenorio [2015], is also used in the analysis. Data on civilian casualties are provided by Condra and Shapiro [2012].

Empirical Strategy

Did legitimate tips received by British forces through the 130 hotline during the Iraq war enable them to carry out successful operations despite persistent efforts by insurgents to overwhelm the line? The relationship between wartime informing and insurgent attacks is complex. In levels, insurgent violence and information are likely endogenous: although intelligence provided by civilians might result in reductions in insurgent violence, areas and/or periods of time in which relatively great amounts of insurgent violence were carried out might tend to be associated with greater information flow because there was simply more information available for citizens to report. Thus, the relationship between levels of tips and insurgent violence is ambiguous.

A more credible strategy for identifying the general effect of ICT-enabled informing on the production of insurgent violence begins by controlling for general trends in both variables by expressing them in differences before regressing a vector of past tips values on the present value of insurgent violence.

Before introducing particular models, I first explore the data. Because the data are high frequency, I first test for non-stationarity and seasonality during the primary time series. Auto-correlation functions of the primary variables of interest (tips, insurgent violence (which can be subdivided by attack type), and counterinsurgency successes (the discoveries of weapons caches and of improvised explosive devices (IED)) show that some of these viables are clearly non-stationary while others exhibit in seasonality. (See the correlograms in Figure 20.) When these variables are differenced, however, all appear stationary, and, with one major exceptions, do not tend to display
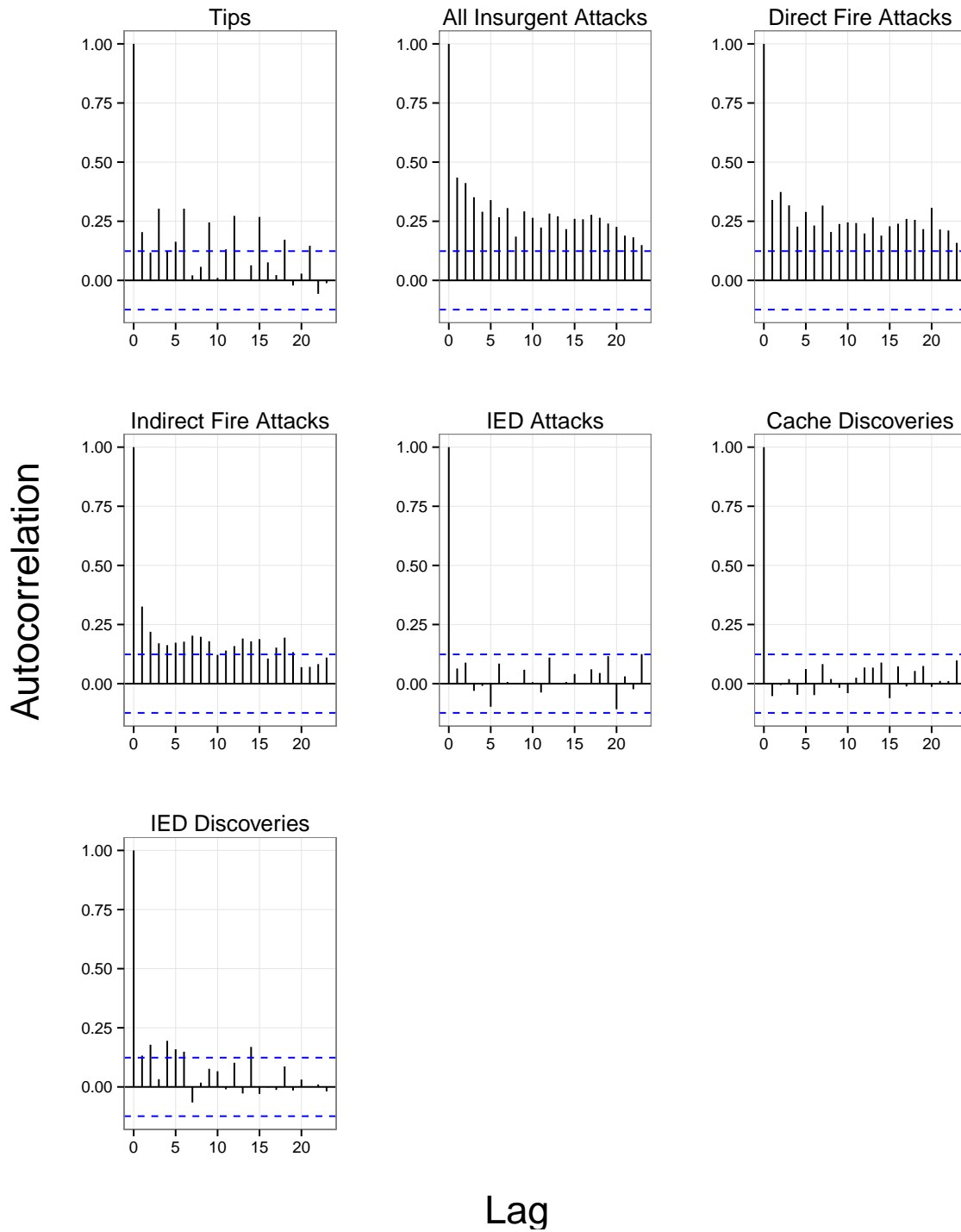
seasonality (see Figure 21).[10]

Figure 20: Autocorrelation Functions of Primary Model Variables in Levels, Primary Time Series

---

[10]ACFs are also generated for the same primary variables for the more limited 2009 time series. However, for that time series, whether variables are expressed in levels or differences no statistically significant trends are apparent. See Figures 22 and 23.
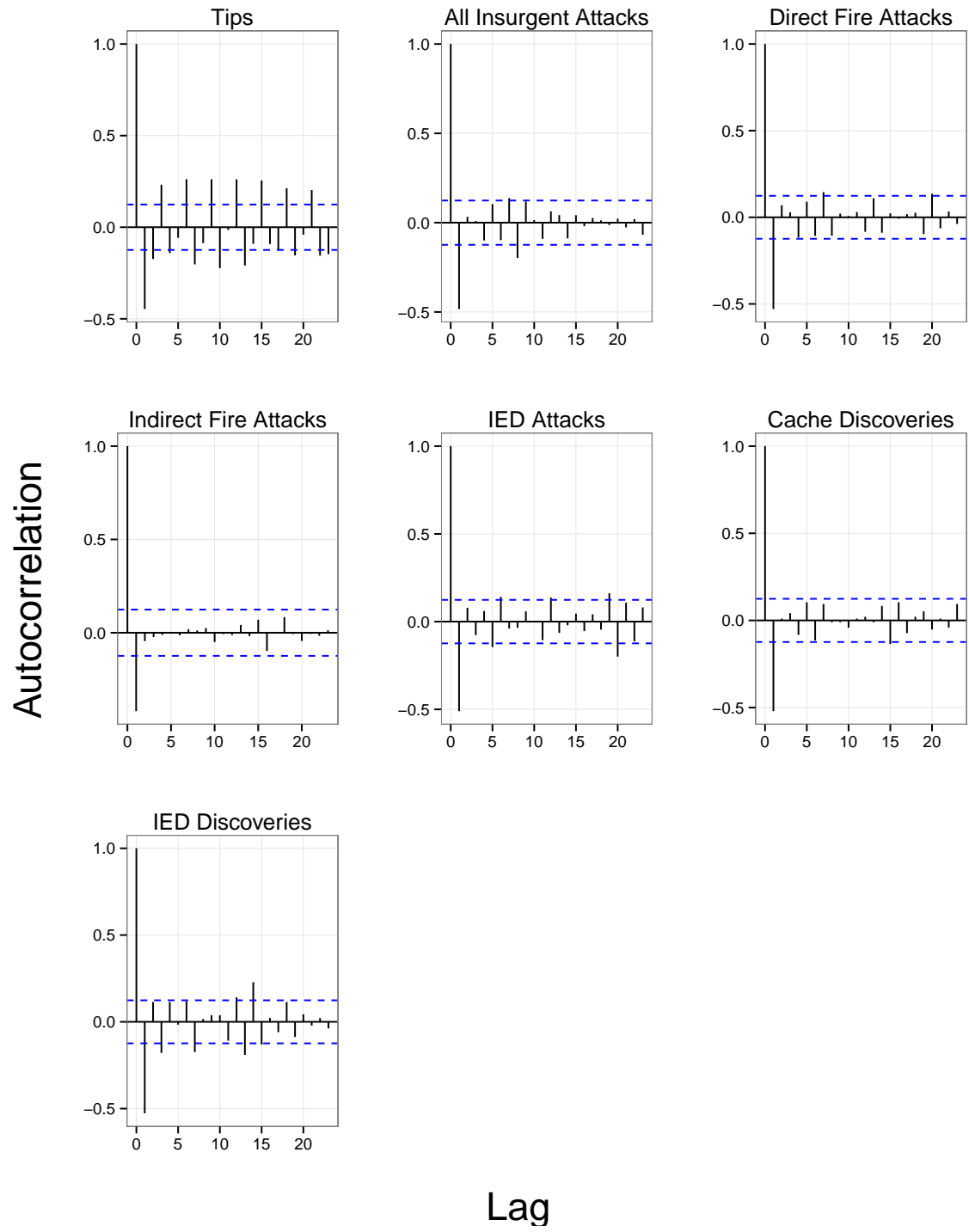
Figure 21: Autocorrelation Functions of Primary Model Variables in Differences, Primary Time Series
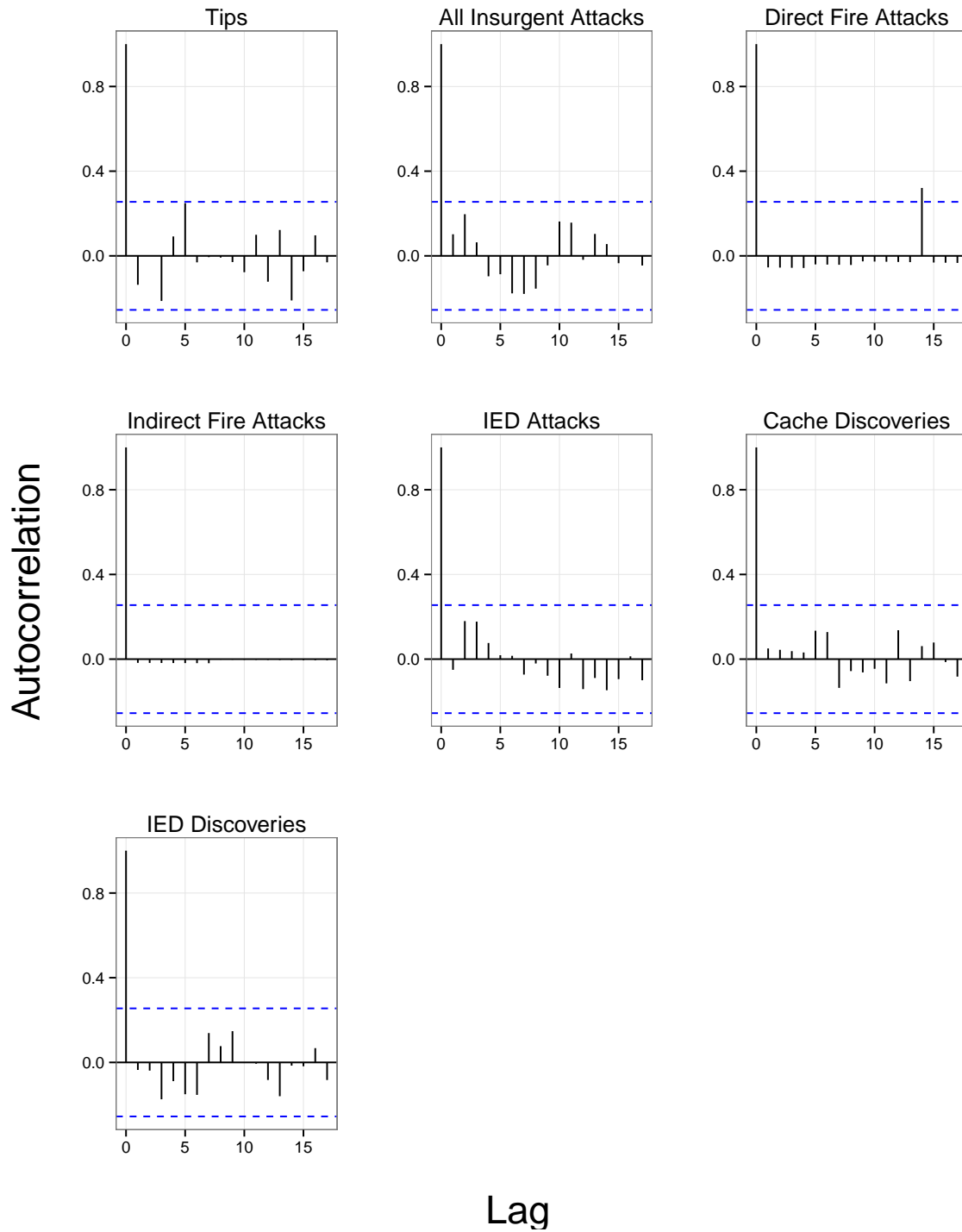
Figure 22: Autocorrelation Functions of Primary Model Variables in Levels, 2009 Time Series
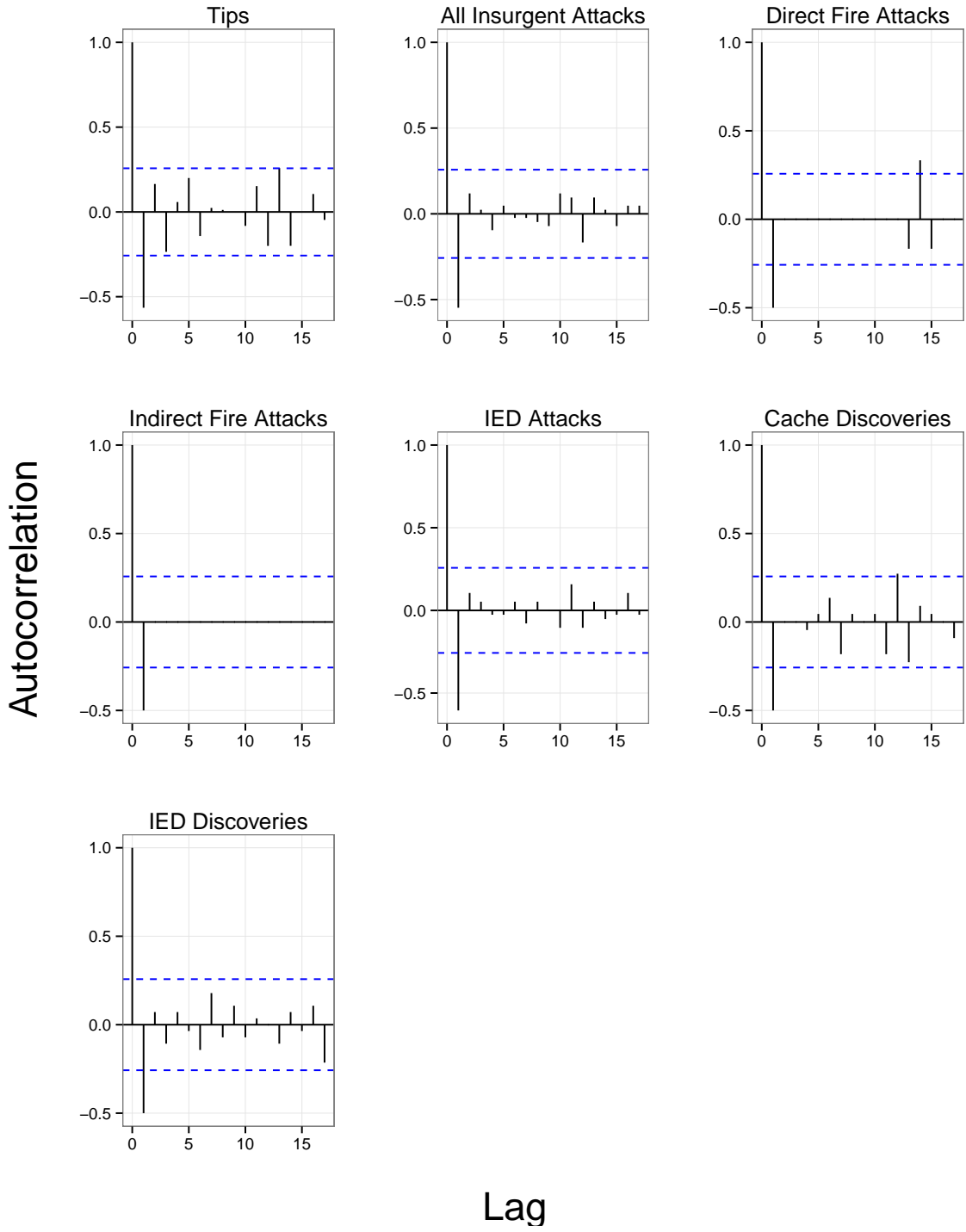
Figure 23: Autocorrelation Functions of Primary Model Variables in Differences, 2009 Time Series

The primary exception is the Δ tips variable, which displays highly persistent three-day cyclicality. This trend persists even when the second- and third-order differences are applied. A clue as to the possible source of this autocorrelation appears in the British records, which indicate

that three separate "shifts" rotated across days (e.g. shift "A" was assigned to June 08, 2006, June 11, 2006, June 14, 2006...; shift "B" was assigned to June 09, 2006, June 12, 2006, June 15, 2006...; etc.). Some heterogeneity in either the number or classification of calls received appears to be attributable to the individual shifts [11] I, therefore, deseasonalize this variable using periodic regression, following Shumway and Stoffer [2006, p. 72], before differencing the regression residuals:

$$\Delta T_t = \alpha_0 + \alpha_1 cos(2\pi w_1 t) + \beta_1 sin(2\pi w_1 t) + \varepsilon_t \tag{1}$$

where the frequency w_1 is set to 1/3. As Table 1 shows, the $cos(2\pi w_1 t)$ variable explains a significant portion of the variation in the differenced variable, and the autocorrelation function of the deseasonalized, differenced variable, although not entirely free of statistically significant lagged values, appears much more reasonable (Figure 24). Thus, in the following discussion on model selection, a differenced deasonalized tips variable is used in place of a differenced-only variable.

---

[11]A similar three-day seasonal pattern is apparent in the spurious call variables as well.
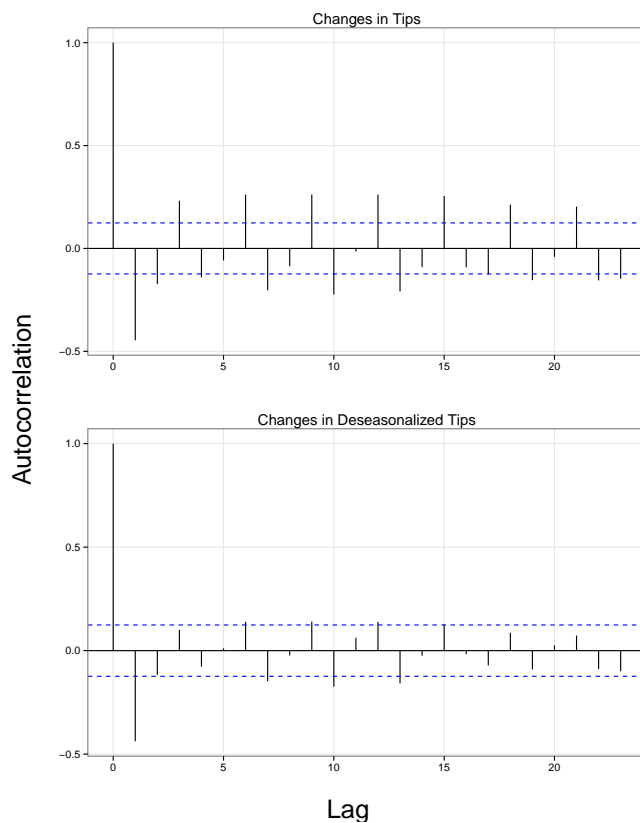
Figure 24: Autocorrelation Functions of Differenced Tips Variable and Differenced Deasonalized Tips Variable Compared, Primary Time Series

Table 1: Periodic Regression Results

	ΔTips
$cos(2\pi\frac{1}{3}t)$	1.109***
	(0.246)
$sin(2\pi\frac{1}{3}t)$	−0.007
	(0.245)
Constant	4.180***
	(0.174)
Observations	251
R^2	0.076
Adjusted R^2	0.068

*p<0.05; **p<0.01; ***p<0.001

33

Because counterinsurgents are likely to act on any information secured through tips relatively quickly, I adopt the day as the unit of analysis and a two-week period of lags. Formally,

$$\Delta V_t = \zeta + \sum_{j=1}^{14}(\vartheta_j \Delta T_{t-j}) + \varepsilon_t \qquad (2)$$

where V and T denote insurgent violence and tips, respectively.

Changes in violence might nonetheless influence changes in tip giving through the former's effect on civilian casualties. Specifically, Shaver and Shapiro [2016] show that civilians during the Iraq war tended to increase (decrease) the number of tips they supplied to Coalition forces following civilian deaths caused by insurgent (Coalition) forces. On days in which there are spikes in violence, the likelihood of civilian collateral damage may increase. Thus, a first modification to the model involves controlling for previous changes in civilians casualties, distinguishing between those for which Coalition forces were blamed and those for which insurgents bore responsibility: $\sum_{j=1}^{14}(\gamma_j \Delta C_{t-j} + \eta_j \Delta I_{t-j})$.

Because differences in insurgent violence are likely to correlate across time, I supplement this time-series model with previous values of insurgent violence. To control for differences across time horizons longer than a one-week period that might account for an observed relationship between the variables, I introduce week fixed effects. Because illegitimate calls placed by the insurgency to the tips hotline may correlate with both insurgent violence and legitimate calls, I include a vector of past values of false calls (the summation of malicious, nuisance, and erroneous calls): $\sum_{j=1}^{14} \zeta_j \Delta F_{t-j}$. I aggregate the three type of spurious calls to limit the total number of model parameters. The dataset contains only 310 total observations, and introducing fourteen days of lags in false calls imposes 28 fewer parameters on the model than if lags of all three call types were introduced separately. Finally, I include a vector of forwarded tips values. Standard errors are heteroskedasticity and autocorrelation consistent.

The full model can be expressed as follows:

$$\Delta V_t = \zeta + \sum_{j=1}^{14}(\vartheta_j \Delta T_{t-j} + \gamma_j \Delta C_{t-j} + \eta_j \Delta I_{t-j} + \zeta_j \Delta F_{t-j} + \xi_j \Delta V_{t-j} + \psi_j \Delta T_{t+j}) + \varphi_w + \varepsilon_t \qquad (3)$$

How should the results of this analysis be interpreted? If insurgents succeeded in drawing British and Iraqi forces into ambushes and/or diverting those forces as they carried out attacks elsewhere in the city, changes in tips should be associated with general increases in insurgent attacks. If insurgents succeeded only in overwhelming the tips lines so that counterinsurgent forces generally lacked timely information with which to act on tips received, no such association (either positive or negative) is expected.

The more complicated case is the one in which the tips line generated a supply of credible intelligence that offset any countervailing efforts by insurgents to manipulate the line. In this case, although increases in information may have benefited counterinsurgents through ultimate reductions in insurgent violence, in the immediate term (the days immediately following counterinsurgents' receipt of information) credible tips might nonetheless be associated with increases in violence. This is because as counterinsurgents act on the information they have obtained, they may come under fire (as they conduct raids, carry out capture/kill operations, and so forth).

To probe the relationship between information supply and battlefield outcomes more closely, I replicate the analysis above, substituting general insurgent violence with the following specific categories of insurgent violence – direct fire attacks (small arms fire attacks, rocket-propelled grenade attacks, etc.); indirect fire attacks (mortar attacks, rocket attacks, etc.); and improvised explosive device (IED) attacks (typically, roadside bomb attacks).

In cases in which counterinsurgent forces have been ambushed or diverted, weak increases in each of these types of violence are likely. For instance, direct fire attacks and/or IEDs might be used in planned ambushes of responding forces. Indirect fire attacks might be carried out during periods of diversion. However, in cases in which counterinsurgent forces act on credible tips, unsuspecting insurgents should have little or no time to respond with IED or indirect fire attacks. Instead, in such cases, immediate increases in direct fire violence would be expected as insurgents engage with raiding counterinsurgent forces in close-quarter engagements. However, reductions in these other forms of violence would be expected as counterinsurgent forces ultimately succeeded in removing insurgents from the battlefield, recovering their weapons, etc.

In this series of attack-type specific regressions, controls for previous values of the other attack

types are included as well since attacks of these various classes are likely to be correlated with one another as well as with information flow.

A final means of probing the effect of the tips hotline involves assessing changes in IED and weapons cache discoveries. If counterinsurgents benefitted from positive changes in the number of legitimate tips received, such relationship should be observed not only through reductions in insurgent violence but through intervening variables such as the discovery of weapons caches and IEDs emplaced along roadways. I, therefore, replicate the analysis a final time, substituting, independently, changes in cache discoveries and in IED discoveries. In these models, I control for IED discoveries in the cache discoveries model and *vice versa*.

Results

Primary results are presented as coefficient plots in Figure 25. Changes in aggregate insurgent violence are generally uncorrelated with past changes in tips; although, days immediately following increases in tips are weakly associated with increases in violence. Within the week following a positive change in information flow, significant positive changes in direct fire attacks are documented by British forces. While such finding is consistent with the possibility that insurgents were effective in drawing counterinsurgent forces into attacks, it is also consistent with the expectation that counterinsurgents entered into firefights as they acted on legitimate tips.

However, results of the regressions when alternative outcomes are used paint a much clearer picture. Changes in indirect fire and IED attacks negatively associate with positive changes in tips. Roughly one week after additional information is received by counterinsurgent forces, reductions in both attack types are observed. Moreover, these reductions are consistent with changes observed in the discoveries of both IEDs and weapons caches. For both variables, positive changes in tips are associated with immediate and persistent increases in the discovery of both items over the two-week period.

These results may nevertheless understate the role of the tips hotline in reducing insurgent violence for two reasons. First, not all quality tips received by counterinsurgent forces are likely to lead to immediate counterinsurgency successes. Consider, for instance, the description of credible

tips received by British forces during the week of March 21st of 2007. Although just over half of these (56%) dealt either with "suspicious activity" or "terrorist/insurgency [activity]", those related to "general crime", "murder", and "dead bodies" made up most of the remaining. Although tips related to this latter class of activities might ultimately result in counterinsurgency successes (after, for instance, investigations into the murder reports and dead body sightings are carried out), they are unlikely to do so over the very short term.

Thus, although the estimated effect of positive changes in credible tips received on, for instance, changes in future IED attacks is negative, if only half of quality tips received permit counterinsurgent forces to carry out near-immediate operations (within, say, the two-week period following receipt of a tip – the type this paper is most concerned with), the estimated magnitude is likely biased toward 0 by "good" tips that provided counterinsurgents with useful information but could not have been used to prevent attacks in the one-to-two week period following their receipt).[12].

Second, the results do not account for possible well-placed informants who were recruited after making initial calls to the hotline but were subsequently directed to use other means of communication to continue to supply intelligence. As one of the U.S. Defense Department describes, when a call came into the primary 130 hotline call center, "hand written reports [were] translated by local national linguists and entered into a database. The translated report [was] given to British contractors under Armor Group who are prior CT Officers from Northern Ireland and were tasked to train and mentor the operators. They have developed their own program for HUMINT sourcing that has Iraq NIIA leadership awareness, but currently no Iraqi involvement. Each caller is asked if they would agree to being called back. If they agree, Armor Group contractors analyze the report to see if they are interested in developing the caller as a source. The Armor Group Brits make initial re-contact and, following 2-3 source meetings will determine if the caller is useful – a vetting process. If so, they will hand off the source to either the Strategic Counter Intelligence Directorate (SCID) or Task Force (TF) 24" U.S. Central Command, U.S. Department of Defense [2007].

---

[12]Unfortunately, daily tips cannot be divided by type. Otherwise, additional statistical analyses could be performed to explore this possibility. Only approximately one dozen weekly reports provided by the UK's Ministry of Defence provide dissaggregate tips details. They are, however, consistent with one another. Typically, less than half of quality tips received are related to "suspicious activity" or "terrorist/insurgency [activity]."
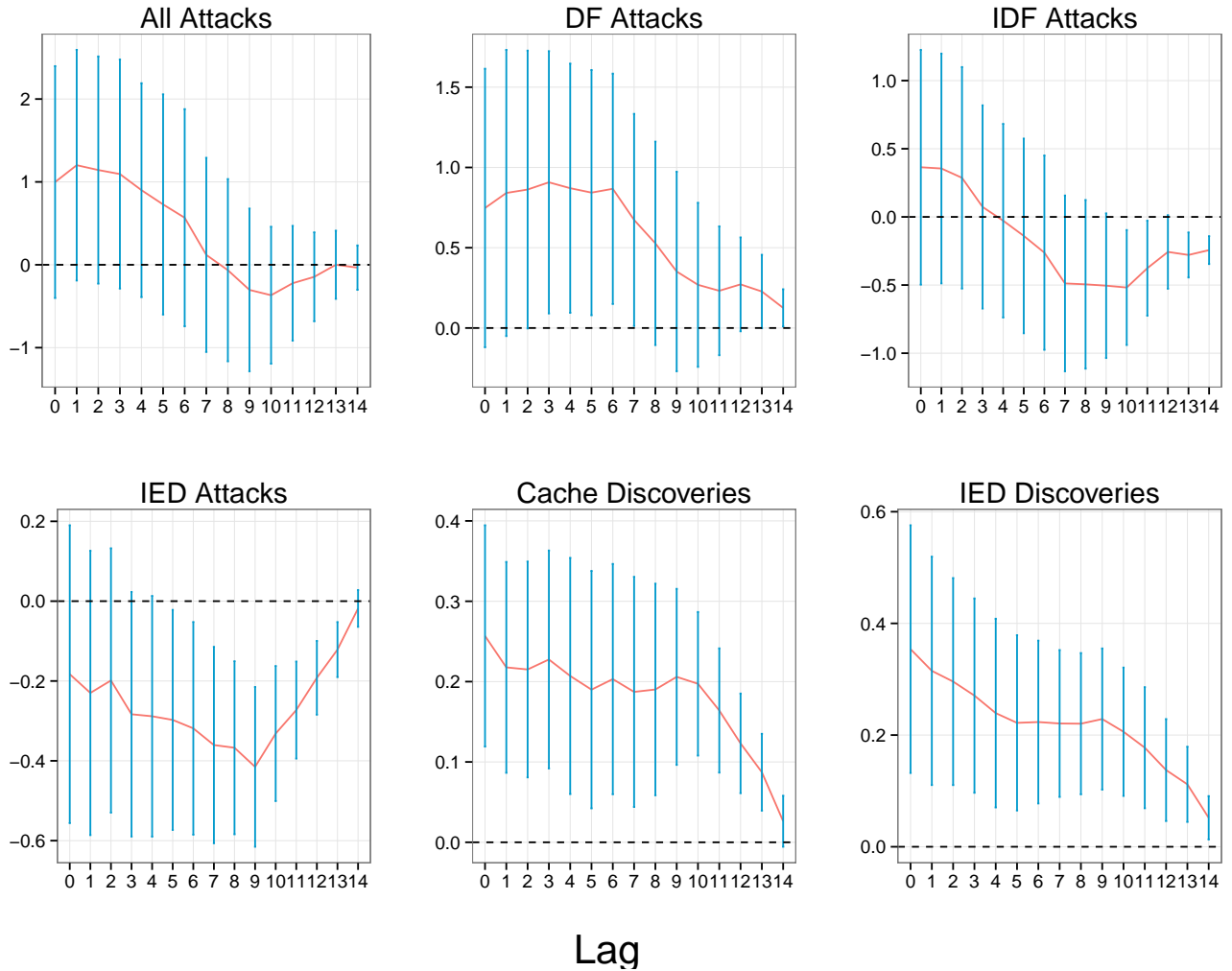
Figure 25: Lagged Changes in Tips on Changes in Outcomes of Interest

Robustness

Sensitivity to Time Period

As Figure 18 shows, during the time period covered in the 2009 time series, the number of false calls (relative to tips) had decreased significantly. By then, the highly organized insurgent operation that was active during the earlier years of the war was no longer active. Were British forces simply more effective during this later period in responding to tips received, either because they had far fewer false tips to sort through or because the insurgents who remained active during this period were less formidable opponents? If so, are the results of the primary model driven by observations from this later period? Rerunning the same set of regressions using only data from

the 2006-07 period shows that this is not the case. The results, which appear in Figure 26, are almost entirely unchanged. Estimated coefficients retain the approximate values of the originals. In several cases (most notably, direct fire and IED discoveries) confidence intervals widen, which is unsurprising given that nearly 20% of the observations are dropped for this analysis.
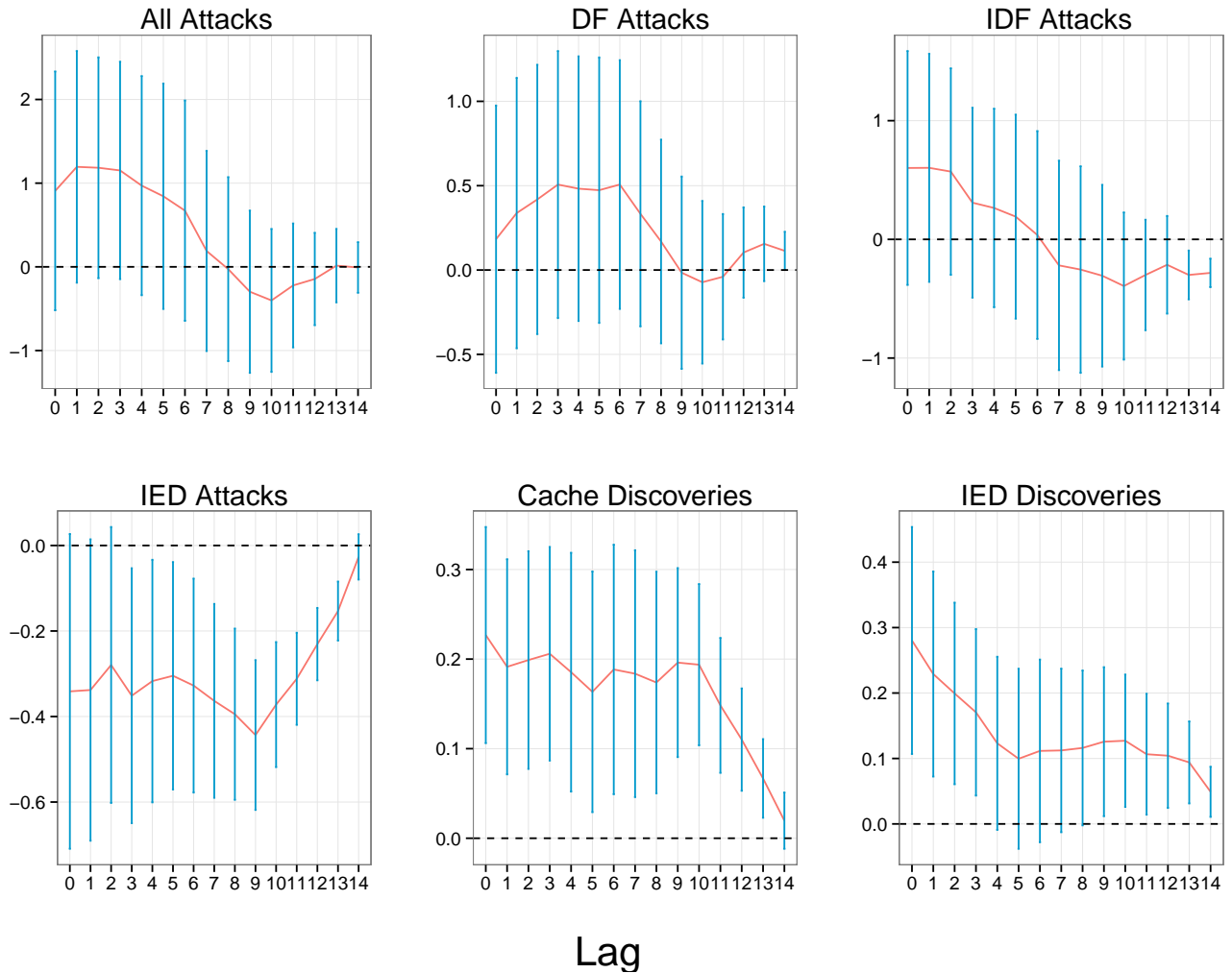

Figure 26: Lagged Changes in Tips on Changes in Outcomes of Interest, Data Sub-Sample

Possible Meteorological Confounders

Tipping and violence might share a correlation on any given day with meteorological variables. For instance, in Iraq, summertime temperatures reach extreme highs, and oppressive temperatures might both drive down violence by limiting insurgents' activities as well as the number of tips reported, both because there are fewer insurgent activities to observe and because citizens are

less likely to be outdoors during such periods. Similarly, sandstorms are common in Iraq. When visibility is diminished, particular types of insurgent activity (like direct fire and IED attacks) might be affected because, for instance, targets are more difficult identify. Similarly, during such periods tipping might fall because there are fewer activities to be observed (either because the number of actual activities has fallen or because citizens simply observe fewer of them).

To ensure that any such relationships do not confound results, I supplement the model with a vector of meteorological controls – specifically, daily maximum temperature, daily maximum temperature squared[13], mean visibility, dew point, and wind speed. These variables are taken from the National Climatic Data Center, National Oceanic & Atmospheric Administration [2016]. Meteorological data is available only for the dates covering the first time series of tips call-center data. This modification is, therefore, carried out as a robustness test rather than serving as the primary model specification.

With one exception, results of this analysis are near perfectly consistent with the primary model results. Results regarding all outcomes of interest except direct fire attacks are unchanged. Whereas the primary model results reveal a significant positive relationship between present changes in direct fire attacks and previous changes in tips, this relationship is attenuated when the meteorological controls are added.

Placebo Test

If the relationship identified between changes in tip flow and subsequent changes in insurgent violence is the result of the theorized causal process, there is no reason to expect that such relationship should persist if the time series is randomized by day before changes in tips are lagged and regressed on changes in insurgent violence and IED and cache discoveries. As expected, the results of this placebo test fail to produce any observable relationship between lagged changes in tips values and present changes in insurgent violence (irrespective of type) and in IED and cache discoveries. These results appear in Figure 27.

---

[13]A squared term is included to account for possible non-linear trends in temperature and violence – for instance, violence might tend to increase in temperature at lower levels but diminish at extreme temperatures.
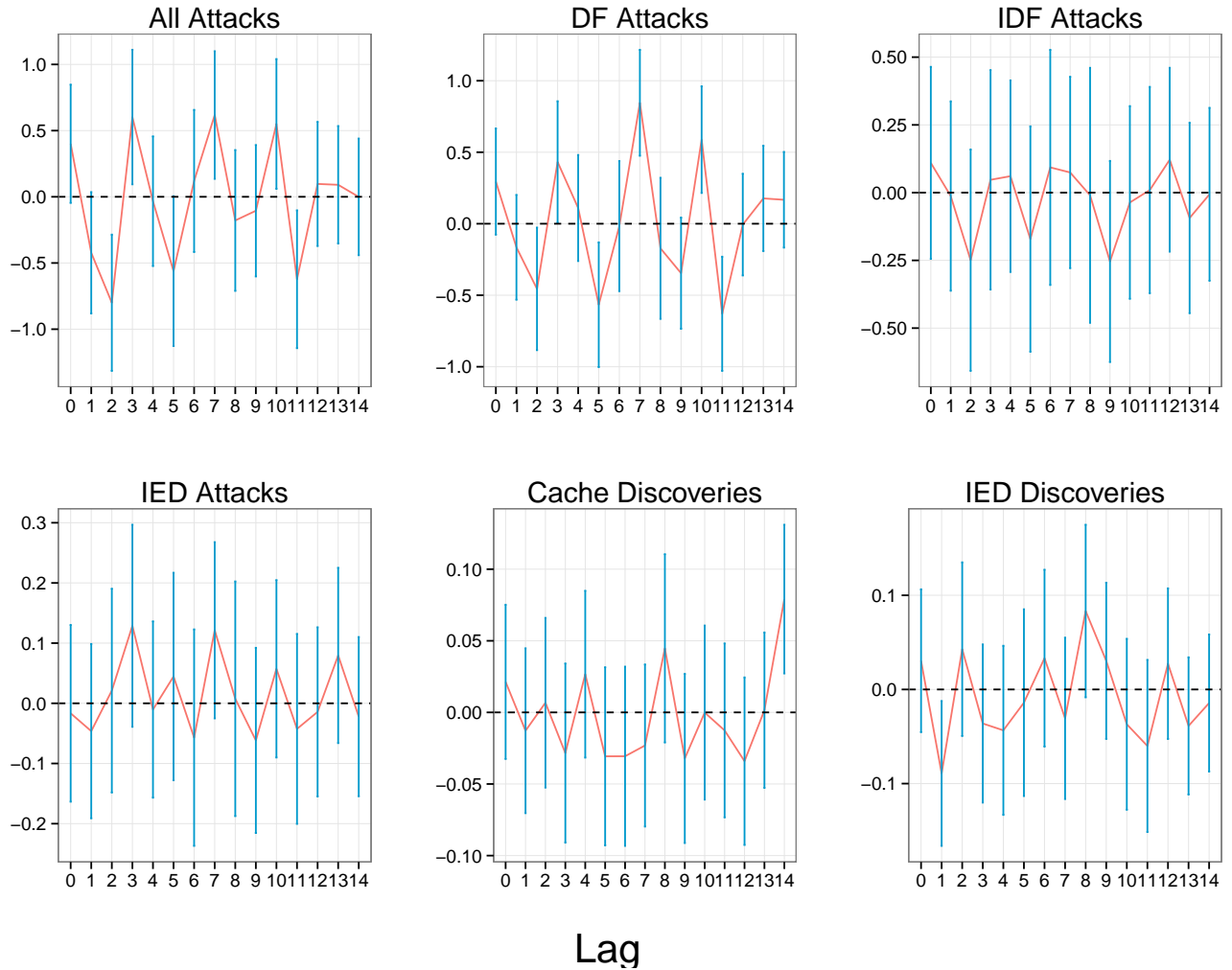
Figure 27: Lagged Changes in Tips on Changes in Outcomes of Interest, Placebo Test

Conclusion

Despite considerable effort by Iraqi insurgents to overwhelm the tips hotline managed by British forces in the country's south, the limited but steady stream of credible information to call center operators appears to have provided British forces with sufficient information to disrupt insurgent activities. While informing through ICT channels during the Iraq war does not appear to have affected changes in overall insurgent violence, the evidence suggests that it was responsible for significant reductions in indirect fire and, in particular, IED attacks. Citizen tips appear to have led British forces to both unexploded roadside bombs, which they then cleared, as well as to weapons caches.

While ICT platforms may tend to favor the efforts of non-state actors to mobilize against more powerful state targets, the results of this analysis suggest that once conflict is initiated, such technologies can benefit the state by upsetting the information asymmetry upon which rebels often rely. Furthermore, this piece offers the first direct quantitative evidence using actual "tips" data of the centuries-old proposition that information plays a central role during insurgency contests.

Can these results be generalized? The American and British militaries are amongst the most technologically sophisticated in the world. That these forces were apparently unable to counter repeated telephony denial of service attacks is informative. If these forces were unable to do so, barring any significant changes in available technologies, it is unclear that governments with access to even fewer technical capabilities would fare any better.

Nevertheless, British forces' apparent success in using the credible information that they did receive may not be generalizable. As Shaver and Shapiro [2016] have noted previously, while it "is a common trope that most intrastate conflicts involve a dramatic discrepancy in military power... the scale of the discrepancy in Iraq during the study period was unusually large... [C]ounterinsurgents forces writ large were highly mobile... and benefited from levels of intelligence support, logistical capacity, and precision indirect fire power... that far exceeded what is available to most states fighting insurgencies. Those capacities enabled them to effectively target any position in space at nearly any time if they had actionable intelligence."

Less capable governments fighting their own insurgencies may find that their inability to limit insurgent efforts to overwhelm tips platforms as well as to react with sufficient speed and force when credible information is received ultimately limit the value of ICT platforms.

References

Tanya Acheson. Inla faction admit falls road shooting. *Belfast Telegraph*, 1996.

Army Sustainment Command, U.S. Department of the Army. *Standard Form 1449 for Contract W91GY0-10-C-0012*. U.S. Department of the Army, 2010.

BBC. One day in iraq: Media and comment. *British Broadcasting Corporation*, 2005.

Eli Berman, Jacob N Shapiro, and Joseph H Felter. Can hearts and minds be bought? the economics of counterinsurgency in iraq. *Journal of Political Economy*, 119(4):766–819, 2011.

Sue Coates. private interview, 2014.

Luke N Condra and Jacob N Shapiro. Who takes the blame? the strategic effects of collateral damage. *American Journal of Political Science*, 56(1):167–187, 2012.

Allan Dafoe and Jason Lyall. From cell phones to conflict? reflections on the emerging ict–political conflict research agenda. *Journal of Peace Research*, 52(3):401–413, 2015.

Daily Sabah. Turkey adds a new emergency call number to its hotline list for 'denouncing terrorists'. *Daily Sabah*, 2015.

David Epstein. How dea agents took down mexico's most vicious drug cartel. *The Atlantic*, 2016.

FRANCE 24. France's 'anti-jihad' hotline gets results. *FRANCE 24*, 2014.

David Galula. *Counterinsurgency warfare: theory and practice.* Greenwood Publishing Group, 2006.

Jim Garamone. Trends positive in baghdad, joint staff general says. *American Forces Press Service*, 2007.

GMA News Online. Nbi sets up hotline to receive terrorism tips. *GMA News Online*, 2010.

Deborah Haynes. Dial m for murder — where one quick call can save a life. *The Times*, 2007.

Philip N Howard, Aiden Duffy, Deen Freelon, Muzammil M Hussain, Will Mari, and Marwa Mazaid. Opening closed regimes: what was the role of social media during the arab spring? *Available at SSRN 2595096*, 2011.

General Irish Republican Army. *Handbook for Volunteers of the Irish Republican Army: Notes on Guerrilla Warfare.* Paladin Press, 1985.

Stathis N Kalyvas, Peter Lange, Robert H Bates, Ellen Comisso, Peter Hall, Joel Migdal, and Helen Milner. The logic of violence in civil war. 2006.

Bernard Kerik. Interim iraqi minister of interior. private interview, 2014.

Nathan Leites and Charles Wolf Jr. Rebellion and authority: An analytic essay on insurgen conflicts. Technical report, RAND Corporation, 1970.

Jason Lyall and Isaiah Wilson. Rage against the machines: Explaining outcomes in counterinsurgency wars. *International Organization*, 63(01):67–106, 2009.

Jason Lyall, Yuki Shiraito, and Kosuke Imai. Coethnic bias and wartime informing. *The Journal of Politics*, 77(3):833–848, 2015.

Richard Macauley. China has created a hotline you can use to report a suspected spy. *QUARTZ*, 2015.

Marco Manacorda and Andrea Tesei. *Liberation Technology: Mobile Phones and Political Mobilization in Africa.* Princeton University Information, Communication, Technology (ICT) and Governance Workshop, 2016.

Donna Miles. Hotline succeeding in foiling iraqi insurgents. *Armed Forces Press Service*, 2004.

Multi-National Corps – Iraq. *MNC-I Tips Report.* U.S. Central Command, U.S. Department of Defense, 2008.

Multi-National Force – Iraq. *MNF-I Statistics Seminar.* U.S. Central Command, U.S. Department of Defense, 2007.

National Climatic Data Center, National Oceanic & Atmospheric Administration. Federal climate complex, global surface summary of day data ftp://ftp.ncdc.noaa.gov/pub/data/gsod/readme.txt. 2016.

Cathy Otten. Yazidis get revenge on isis in sinjar. *The Daily Beast*, 2015.

Pakistan Hotline. Call pakistan army hotline 1135 in case of terrorism emergency. *Pakistan Hotline*, 2014.

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

Mitchell Prothero and Susannah George. Coalition success seen in islamic state's cutoff of cellphone service in mosul. *McClatchyDC*, 2014.

Jacob N Shapiro and David A Siegel. Coordination and security how mobile communications affect insurgency. *Journal of Peace Research*, page 0022343314559624, 2015.

Jacob N Shapiro and Nils B Weidmann. Is the phone mightier than the sword? cellphones and insurgent violence in iraq. *International Organization*, 69(02):247–274, 2015.

Andrew Shaver and Jacob Shapiro. The effect of civilian casualties on wartime informing: Evidence from the iraq war. *Households In Conflict Network Working Paper n. 210*, 2016.

Andrew Shaver and Gabriel Tenorio. Public goods provision and information sharing during insurgency. *Princeton University, unpublished manuscript*, 2015.

Harriet Sherwood and Hazem Balousha. Hamas kills 21 suspected informers. *The Guardian*, 2014.

Nouman Shubbar. Iraq ministry of interior police adviser. private interview, 2016.

Robert H Shumway and David S Stoffer. *Time series analysis and its applications: with R examples.* Springer Science & Business Media, 2006.

Marlise Simons. Peru adopts severe tactics to combat guerrillas. *The New York Times*, 1984.

Stephen Smith. Chemicals signal change of tactics in iraq. *CBS News*, 2007.

Stanford University & NYU. under drones, living, 2012.

Zachary Steinert-Threlkeld. *Spontaneous Collective Action: Peripheral Mobilization During the Arab Spring.* Princeton University Information, Communication, Technology (ICT) and Governance Workshop, 2016.

Task Force Baghdad PAO. Iraqi tip saves lives, coalition forces prevent attacks. *Digital Video and Imagery Distribution System*, 2005.

First Iraqi tips line operator. Iraq ministry of interior official. private interview, 2014.

UK Ministry of Defence. *Tips Hotline, Basrah –Weekly Report*. UK Ministry of Defence, 2007a.

UK Ministry of Defence. *TIPS Hotline – Weekly Report – May 17 - May 23 2007*. UK Ministry of Defence, 2007b.

UK Ministry of Defence. *Tips Reporting Procedures*. UK Ministry of Defence, 2016.

U.S. Central Command, U.S. Department of Defense. *E-Mail Exchange*. U.S. Central Command, U.S. Department of Defense, 2006.

U.S. Central Command, U.S. Department of Defense. *Point Paper*. U.S. Central Command, U.S. Department of Defense, 2007.

U.S. Department of Defense. Measuring stability and security in iraq – december 2007. 2007.

Nils B Weidmann. A closer look at reporting bias in conflict event data. *American Journal of Political Science*, 2015.