

ONLINE APPENDIX A:  
Data, Methods and Robustness Checks

“Invisible Digital Front:  
Can Cyber Attacks Shape Battlefield Events?”

*Journal of Conflict Resolution*

Nadiya Kostyuk & Yuri M. Zhukov  
University of Michigan

September 19, 2017

**Contents**

<b>1</b>	<b>Cyber operations data (Ukraine)</b>	<b>3</b>
1.1	Classification and description of cyber operations data . . . . .	3
<b>2</b>	<b>Violent events data (Ukraine)</b>	<b>7</b>
2.1	Training Set . . . . .	10
2.2	Intercoder reliability . . . . .	14
2.3	Support vector machine . . . . .	15
<b>3</b>	<b>Holidays and other political events (Ukraine)</b>	<b>16</b>
<b>4</b>	<b>Variable descriptions for aggregated data (Ukraine)</b>	<b>17</b>
4.1	Geographic locations and dates . . . . .	17
4.2	Kinetic operations . . . . .	18
4.3	Cyber operations . . . . .	18
4.4	Explanatory variables . . . . .	18
<b>5</b>	<b>Summary statistics (Ukraine)</b>	<b>19</b>
<b>6</b>	<b>Cyber operations data (Syria)</b>	<b>19</b>
6.1	Classification and description of cyber operations data . . . . .	20
<b>7</b>	<b>Violent events data (Syria)</b>	<b>23</b>

<b>8</b>	<b>Variable descriptions for aggregated data (Syria)</b>	<b>23</b>
8.0.1	Geographic locations and dates . . . . .	23
8.0.2	Kinetic operations . . . . .	23
8.0.3	Cyber operations . . . . .	23
8.0.4	Explanatory variables . . . . .	24
<b>9</b>	<b>Holidays and other political events (Syria)</b>	<b>24</b>
<b>10</b>	<b>Robustness checks</b>	<b>25</b>
10.1	Test 1: All cyber and kinetic operations in Ukraine from August 17, 2013 to February 29, 2016 . . . . .	27
10.2	Test 2: ‘Propaganda’ cyber operations and physical violence in Ukraine from August 17, 2013 to February 29, 2016 . . . . .	31
10.3	Test 3: ‘Disruption’ cyber operations and physical violence in Ukraine from August 17, 2013 to February 29, 2016 . . . . .	35
10.4	Test 4: ‘Disruption’ & ‘both’ cyber operations and physical violence in Ukraine from August 17, 2013 to February 29, 2016 . . . . .	39
10.5	Test 5: Cyber and kinetic operations during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015) . . . . .	43
10.6	Test 6: ‘Propaganda’ cyber operations and physical violence during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015) . . . . .	47
10.7	Test 7: ‘Disruption’ cyber operations and physical violence during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015) . . . . .	51
10.8	Test 8: ‘Disruption’ & ‘both’ cyber operations and physical violence during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015) . . . . .	55
<b>11</b>	<b>Syria Results &amp; Robustness Checks</b>	<b>62</b>

## 1 Cyber operations data (Ukraine)

Our cyber event data on Ukraine include 1,841 unique cyber attacks from 27 August 2013 to 29 February 2016. These data draw on two sets of sources. First are media reports of cyber attacks from rebel, Russian, Ukrainian, and Western media news outlets, press releases and blogs, along with social media platforms used by the involved non-state actors. 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/computer-security (*Arstechnica*, *Digital Dao*, *Information Week*, *F-Secure*, *Graham Cluley*, *TechWeek Europe*) and mainstream (*Die Welt*, *Newsweek*, *New York Times*, *Politico*, *Postimees (Estonia)*, *Security Affairs*, *The Christian Science Monitor*) news. To reduce potential false positives due to unconfirmed reports or dubious claims of responsibility, we only included attacks reported by more than one source. When multiple sources of the same background reported the same attack, we included only one source in order to avoid duplication. For instance, sources labeled as “DSP” include Dokukin’s social media pages, as well as various websites and twitter accounts that he references.

Our second source of data are distributed denial of service attacks (DDoS)<sup>1</sup> detected by Arbor Networks, and publicly released as part of the private cyber security firm’s Digital Attack Map (DAM).<sup>2</sup> Unlike the first set of data sources, which includes only the most publicly visible cyber attacks – as reported in open media sources, or as claimed by hacker groups directly – the second set utilizes anonymous attack traffic data between Ukraine and Russia, and network outage reports.

### 1.1 Classification and description of cyber operations data

After cross-checking all cyber events with multiple sources, we classified them using the codebook below.

#### Ukraine Cyber Attacks Codebook

1. ATTACK\_ID
2. DATE (YYYYMMDD format)
3. INITIATOR (partisanship)
  - (a) 1 - pro-Kyiv;
  - (b) 0 - pro-DNR/LNR; pro-Russia.
4. INITIATOR\_UNIT
  - (a) ANU - Anonymous Ukraine;
  - (b) CBT - Cyber Berkut;
  - (c) CRN - Cyber Riot Novorossiia;
  - (d) GDN - Green Dragon;

<sup>1</sup>As defined by Arbor Networks, DDoS attack is “an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.”

<sup>2</sup>Digital Attack Map, built by Google Ideas and Arbor Networks, provides a live data visualization of DDoS attacks around the globe. More information could be found at their website: <http://www.digitalattackmap.com/about/>.

- (e) QDH - Quedagh;
- (f) PRG - Pro-Russian Government Units, including news outlets, such as *Russia Today*, Wikipedia pages; this category only includes individuals that support Russian governments but are not necessarily “separatists or terrorists”; moreover, this category includes private companies that support the actions of the Russian government;
- (g) RAU - Russian Army Unit;
- (h) RSU - Russian State Units, including the *Roskomnadzor*;
- (i) RSS - Russian State-sponsored;
- (j) UAU - Ukrainian Army Unit;
- (k) UCF - Ukrainian Cyber Forces;
- (l) UGO - Ukrainian Government Organization;
- (m) UNK - Unknown; Unspecified;

#### 5. INITIATOR\_STATE

- (a) 1 - State Actor;
- (b) 0 - Non-state Actor;

#### 6. DISPUTED

- (a) 1 - Disputed. In the case when no one claimed responsibility for their actions, such attacks were marked as “disputed.” For instance, despite the circumstantial evidence, the cyberespionage operation *Armageddon* claimed to be conducted by the Russian state is marked as “disputed” since the state never took responsibility for it.
- (b) 0 - Non-disputed. Cyber attacks for which non-state actors claimed responsibility on their social media platforms or in interviews with mass media representatives are labeled “non-disputed.”

#### 7. TARGET (partisanship)

- (a) 1 - pro-Kyiv;
- (b) 0 - pro-DNR/LNG; pro-Russia.

#### 8. TARGET\_UNIT\_1

- (a) CGO- Crimean Government Officials; these attacks include attacks on websites, cell phones, emails, etc;
- (b) OTH - Other; this category includes any other target (e.g. advertisement billboards);
- (c) PRG - Pro-Russian Government Units, including news outlets, such as *Russia Today*, Wikipedia pages; this category only includes individuals that support Russian governments but are not necessarily “separatists or terrorists”; moreover, this category includes private companies and individuals that support the actions of the Russian government;
- (d) PUG - Pro-Ukrainian Government Units, including social media webpages, websites of news outlets, websites with Ukrainian propaganda, TV-channels; this category includes hacking cell phones of the PUG; this category only includes individuals and private companies that support the actions of the Ukrainian government;
- (e) RAU - Russian Army Unit;
- (f) RBG - Rebel Groups, including their cell phones, websites, emails, bank accounts, and servers;
- (g) RSU - Russian State Units and government officials;
- (h) UGO - Ukrainian Government Officials;
- (i) UAU - Ukrainian Army Unit;
- (j) WGO - Western Governments and Organizations (e.g. NATO);
- (k) WNO - Western pro-Ukrainian organizations, including private companies and citizens.

#### 9. TARGET\_UNIT\_2

#### 10. TAGRGET\_STATE\_1

- (a) 1 - State Actor;

- (b) 0 - Non-state Actor;
- (c) TAGRGET\_STATE\_2

## 11. ATTACK\_TYPE\_1

- (a) AVG - collecting audio-, video-, and geo-intelligence; it could be done via hacking into CCTV cameras, listening to conversations, etc;
- (b) BWC - blocking websites via sending/filing complaints to the companies that host those websites;
- (c) CPI - collecting private information via open sources;
- (d) DDS - distributed denial-of-service attack, including TCP SYN floods. It is a “type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. A Denial of Service (DoS) attack is different from a DDoS attack. The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.”<sup>3</sup>
- (e) ODS - other individual attacks with a purpose of disruption or espionage. This category includes drone interception, illegal installation of equipment, usage of malware (software that is intended to damage or disable computers and computer systems)(e.g., Blackenergy) or a malicious code. We combine these attacks into one category because of their low frequency in our data set;
- (f) PPI - publishing online private information of the members of the conflicting parties (e.g. bank account info, DOB, identification codes, addresses, etc);
- (g) PRM - posting pro-Russian/rebel messages on various websites, including those that criticize the present “junta” government in Ukraine;
- (h) PUM - posting pro-Ukrainian messages on various websites, including those with Ukrainian propaganda;
- (i) SPE - spear-phishing email (an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data). This category also includes phishing emails (the activity of defrauding an online account holder of financial information by posing as a legitimate company);
- (j) STM - sending massive text messages or calling phones non-stop;
- (k) UNK - unknown, not specified;
- (l) UWP - updating online pages (e.g., Wikipedia);
- (m) WBG - website blockage is “a process by which a Firewall or WWW Proxy prevents users from accessing some network resources, such as World-Wide Web sites or Ftp servers.”<sup>4</sup> This category also includes blocking websites via sending/filing complaints to the companies that host those websites;
- (n) WDT - website defacement “is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.”<sup>5</sup> This category also include defacement of social media accounts;
- (o) WFC - gaining control of Wi-Fi access points and changing them to those of the opponent’s; also includes network and VoIP devices, routers, FTP servers, and motherboards in Russia, Crimea, and Donbas;
- (p) ZDE - using zero-days exploits. “A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it” this exploit is called a zero day attack.”<sup>6</sup>

## 12. ATTACK\_GOAL\_1 - a purpose of the attack

- (a) PRP - mainly propaganda with a purpose of either to influence public opinion or to hurt financing or recruitment campaigns;
- (b) DSR - disruption, espionage, sabotage, using cyber means;
- (c) BTH - both (propaganda & disruption)

## 13. ATTACK\_TYPE\_2

## 14. ATTACK\_GOAL\_2 - a purpose of the attack

## 15. OPERATION\_NAME

- (a) APS - “Apokalinsys”; the UCF campaign; its main goal is to turn off the rebels’ wireless and wired network devices;

- (b) ARM - “Armageddon,” a cyberespionage operation;
- (c) BJB - “Bond, James Bond”, a campaign by the UCF; its main goal is to collect audio-, video-, and geo-intelligence;
- (d) BNR - “Bende”, a campaign by the UCF; its main goal is to call terrorists and provide them with propagandistic information or threaten them;
- (e) KSM - “Kibershtorm”, a campaign by the UCF; its main goal is to block rebels’ cell-phones by sending a large amount of text messages;
- (f) KS2 - “Kibershtorm-2”, a campaign by the UCF; its main goal is the same as KSM’s – to block rebels’ cell-phones by sending a large amount of text messages; the only difference is the content of the text messages; they usually included threats, disinformation, and propaganda;
- (g) KUK - “Krym - tse Ukraina”, a campaign by the UCF; its main goal is to return control over all Crimean government websites;
- (h) KUN - “Kiberurahan”, a campaign by the UCF; its main goal is to block rebels’ phones by constantly calling them;
- (i) OIC - Operation Independence;
- (j) PHL - “Putin-Huilu” (a tentative name, which was never confirmed); a UCF campaign with the main goal of controlling Wi-Fi access points in Russia, DNR, LNR, and Crimea;
- (k) PNT - “Poliuvannia na troliv”, a campaign by the UCF; its main goal is to block trolls’ social media accounts (e.g. livejournal.com, FB);
- (l) VPD - “Vidnovlennia pravdu,” a campaign by the UCF; its main goal is to update Wikipedia pages with accurate (often pro-Ukrainian) messages;
- (m) VPR - “Vymknytu propahandu”, a campaign by the UCF; its main goal is to block pro-Russian propaganda on various websites, including Youtube; usually the UCF email their complaints to *Youtube* and other hosting companies;
- (n) VPT - “Vidplata”, a campaign by the UCF; its main goal is to block websites by using DDoS attacks;
- (o) ZBV - “Zablokovani vyrodku”, a campaign by the UCF; its main goal is to block rebels’ financial resources by complaining to companies/organizations that host those websites;
- (p) ZNR - “Z Novym Rokom”; the UCF operation; its main goal is to hack printers in the Crimea, Russia, and Donbas, and print pro-Ukrainian messages;

#### 16. REPORTING\_SOURCE\_1

- (a) CBW - Cyber Berkut’s webpages, including their official website (<http://cyber-berkut.org>, <http://pastebin.com>), their page on [vkontakte.ru](http://vk.com/cyberberkut1) (<http://vk.com/cyberberkut1>). It is worth mentioning that the Anonymous Ukraine also uses *pastebin* to post their information;
- (b) CRW - Cyber Riot Novorossiya’ webpages, including their pages in [vkontakte.ru](http://vkontakte.ru) and twitter;
- (c) CSN - Computer-Security News, including *Graham Cluley*, *TechWeek Europe*, *Arstechnica*, *Information Week*, *Digital Dao*, *Computer Weekly*, *Tech News*, *Wired*;
- (d) DAN - DAN News;
- (e) DRG - Dark Reading;
- (f) DSP - Dokukin’s Social Media pages, including those on Facebook and twitter (MustLiveUA twitter page) as well as his website [websecurity.com.ua](http://websecurity.com.ua); it also includes twitter accounts of other users that he refers to;
- (g) FSC - F-Secure;
- (h) GDW - Green Dragon’ webpages, including their pages in [vkontakte.ru](http://vkontakte.ru) and twitter;
- (i) IUK - Interfax Ukraine;
- (j) LGR - Looking Glass Report;
- (k) NWS - Newsweek;
- (l) NYT - New York Times;
- (m) RBH - Russia Beyond the Headlines;
- (n) RNS - Pro-Russian government news sources (e.g. [Vesti.ru](http://Vesti.ru), [Ria Novosti](http://Ria Novosti), [Sputnik](http://Sputnik));
- (o) SGN - Segodnia;
- (p) RKE - Rahn, Khrennikov & Eglitis (2014);

- (q) UGW - Ukrainian governmental website;
- (r) UNO - Ukrainian news outlets, including *RBK-Ukraina*;
- (s) WNS - Western news sources, e.g. *Postimees* (Estonian news source), *Security Affairs*, *The Christian Science Monitor*, *Politico*, *Die Welt*, *Reuters*, *International Business Times*;
- (t) YTB - Youtube;

17. REPORTING\_SOURCE\_2

18. REPORTING\_SOURCE\_3

## 2 Violent events data (Ukraine)

The main article employs two sets of event data: one on physical violence and the second on cyber attacks. The first of these is a dataset of violent incidents from the armed conflict in Ukraine’s Donbas region, previously used by [ANONYMIZED]. For each day between 28 February 2014 and 29 February 2016,<sup>7</sup> the dataset includes information on the number of unique government and rebel operations, their locations, participants, and other event-level details.

The violent event data are based on human-assisted machine coding of news reports, press releases and blog posts from Ukrainian, Russian, rebel and international sources. Ukrainian sources include television channels 112, Channel 5, Espresso.tv, the military blog Information Resistance, and the newswire services Interfax-Ukraine and Ukrinform. Russian sources include the state-owned news channel Russia-24/Vesti, the independent TV channel Dozhd, non-government news websites Gazeta.ru, Lenta.ru, and BFM.ru, and the Russian edition of the Interfax newswire service. Pro-rebel sources include Rusvesna.su, Donetsk News Agency (DAN) and News Front. Also included are the Russian-language edition of Wikipedia, and daily briefings from the OSCE Special Monitoring Mission to Ukraine. For each data source, we created a separate electronic text corpus that contained all incident reports published on the Donbas in these 17 sources since February 2014 ( $N = 72,010$ ).

To determine the geographic locations of events mentioned in the reports, we ran an automated geocoding script that identified populated place names referenced in the text, and matched them against the U.S. National Geospatial Intelligence Agency’s GeoNames database.<sup>8</sup> Table 1 shows the resulting spatial distribution of events, by source.

To determine the content of the incident reports, we used a supervised learning algorithm – Support Vector Machine – to classify each event into a series of pre-defined categories. These categories include event type, initiator, target, tactic, and casualties.

For a report to be classified as a *Ukrainian kinetic operation*, it must involve specific act of organized violence initiated by any pro-Kyiv armed group. A specific act of violence is a reference to a single ongoing or recent military operation, targeted killing, detention, act of terrorism, or

<sup>7</sup>This date range includes the early protest phase of the conflict immediately following the ouster of former president Viktor Yanukovich (March 2014), the initial violent uprising and seizure of government buildings (April 2014), the full-scale combat operations that followed the independence referendum of 11 May 2014, and the second Minsk ceasefire agreement of 15 February 2015.




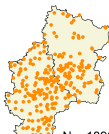


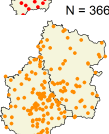
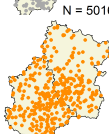
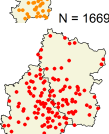
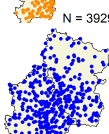
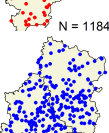
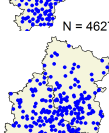
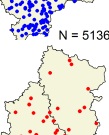
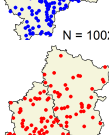
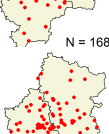
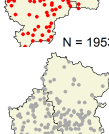
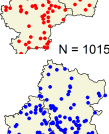
<sup>8</sup>We used a one-to-many mapping algorithm, to account for multiple events mentioned in the same report. To identify and correct geocoding errors and double-counts, each list of geocoded locations was referenced against a lookup table of regular errors (e.g. to ensure that ‘Donetsk oblast’ isn’t mis-coded as ‘Donetsk city,’ and that references to the ‘Shakhtar battalion’ are not mis-coded as ‘Shakhtarsk city’). We also performed manual inspection.

other violent event. Not included in this category are general summaries of war statistics or press statements. Pro-Kyiv groups include Ukraine's regular Army, Air Force, Airborne troops, Marines, Border Guard, SBU, Interior Ministry, local police, National Guard or any of 46 volunteer battalions (e.g. Azov, Aydar, Dnipro-1, Donbas) and independent right-wing militias (e.g. Right Sector).

For a report to be classified as a *pro-rebel kinetic operation*, it must involve organized violence by any anti-Kyiv armed group. Anti-Kyiv groups include any forces explicitly labeled as 'insurgents,' 'rebels,' 'terrorists,' as well as specific formations like the Novorossiia Armed Forces, Donetsk or Lugansk People's Republic (DNR, LNR), Vostok Battalion, Oplot, Kal'mus battalion, Bezler band, Zarya battalion, Russian Orthodox Army, People's Militia of Donbass, Prizrak battalion, Army of the South East, Don Cossacks, Russian National Unity, Eurasian Youth Union, Yovan Sevic. We also labeled references to actions by Russian Armed Forces (mostly in Ukrainian media) as 'rebel.'



Table 1: Sources included in Ukraine dataset

Name	Map	Info	Name	Map	Info
112 (Ukraine)		TV Rus/Ukr-language	Lenta.ru (Russia)		Online Rus-language
Channel 5 (Ukraine)		TV Ukr-language	NewsFront (rebel)		Online Rus-language
BFM (Russia)		Online Rus-language	OSCE (international)		Online English-language
DAN (rebel)		News agency Rus-language	RusVesna (rebel)		Online Rus-language
Dozhd (Russia)		TV Rus-language	Sprotyv (Ukraine)		Online Rus-language
Espresso (Ukraine)		TV Ukr-language	Ukrinform (Ukraine)		News agency Rus/Ukr-language
Gazeta.ru (Russia)		Online Rus-language	Vesti (Russia)		TV Rus-language
Interfax.ru (Russia)		News agency Rus-language	Wikipedia (international)		Online Rus-language
Interfax.ua (Ukraine)		News agency Rus/Ukr-language			

## 2.1 Training Set

For each dataset shown in Figure 1, we and a team of research assistants read a randomly-selected training set of 130-600 reports (depending on the size of the corpus), in Russian, Ukrainian and/or English. The authors and one research assistant read all training set documents in their original languages. Research assistants not fluent in Russian or Ukrainian read training sets containing the same reports, machine-translated into English.

All research personnel received codebook with instructions for event classification. The sections of this codebook relevant to the analysis in the paper is pasted below.

### Training Set Codebook

For this assignment, you will read media reports from Ukrainian and Russian press (translated into English), and classify them by location, actors and tactics. It will require downloading and installing an open-source statistical software package (R), and running a simple program that displays the text of a media report and asks you a series of questions about its content.

Below is a set of instructions on how to open and analyze these data.

1. ... [technical instructions on downloading and installing R]
2. Open the R application.
3. In R console, enter the following lines of code at the '>' prompt:

```
setwd("My Directory")
source("databoom.R")
```

Be sure to change "My Directory" to your actual working directory from (3).

4. You will then be shown a media report on the screen (in Ukrainian, Russian, or translated, sometimes poorly, into English), and will be asked several questions about its content and tone. Here is an example:

```
> setwd("My Directory")
> source("databoom.R")
```

```
[1] "Summary of the United Army of the South-East (at 9.44 MSK). According to her,
early in the morning Ukrainian gunships attacked Belenky near Kramatorsk.
In Donetsk, the Ukrainian military militia broke through roadblocks in Karlivka,
fights go in Netaylovo. In the Lugansk region are fighting in the village
Zheltoye, in the village Metalist (a suburb of Lugansk) and Stanitsa-Luganskaya,
as there are fights in the Krasnyi Partizan (next to Russian Gukovo). Shelling also
began in Snezhnoye and Saur-Mogila."
```

```
1 Violent event? (Y/N)
1 Gibberish / Incomprehensible / Missing text / Foreign Language? (Y/N)
1 INITIATOR: Government/rebel/unknown/civilian/other (G/R/U/C/O)
1 INITIATOR: name of unit? (see list)
1 TARGET: Government/rebel/unknown/civilian/other (G/R/U/C/O)
1 TARGET: name of unit? (see list)
1 TYPE OF ACTION: tactic or weapons system used (see list)
1 CASUALTIES: civilians killed
1 CASUALTIES: civilians wounded
1 CASUALTIES: rebels killed
1 CASUALTIES: rebels wounded
1 CASUALTIES: government killed
1 CASUALTIES: government wounded
1 Comments? (optional)
1 Do you want to re-enter your responses? (Y/N)
1 Additional events in record? (Y/N)
```

Some notes:

- You can enter UPPER CASE or lower case responses ('Y' or 'y')
- If you feel **you have made an error**, you can re-code the event. Toward the end of the questionnaire, you will be asked if you'd like to re-enter your responses. Answer 'Y' (or 'y' or 'yes' or '1') to that question.
- If there are **multiple records per event** (e.g. 'attacks happened in villages A, B and C'), enter each record separately. At the end of each questionnaire, you will be asked if there are additional events in the report. Answer 'Y' (or 'y' or 'yes' or '1') to that question.
- Press 'ESC' to interrupt the program at any time. To continue, type source("databoom.R") in the command window again.
- The program automatically saves your place in the training set. So, if you close R and then restart it, you should start where you left off.

Here is some background on how to respond to these questions.

- **Violent event?** (Y/N)

Answer 'Y' (or 'y' or 'yes' or '1') if the report describes a specific military operation, rebel attack, or other incident of violence. Answer 'N' (or 'n' or 'no' or '0') if the report describes something else, like a general summary of war statistics ('in the two months since April, XXX have been killed'), or a press statement (except for statements that describes specific events).

- **Gibberish / Incomprehensible / Missing text / Foreign Language?** (Y/N)

Self explanatory.

- **INITIATOR: Government/rebel/unknown/civilian/other** (G/R/U/C/O)

Enter G for government, R for rebel, U for unknown, C for civilian, O for other (e.g. Russian armed forces).

Note that Ukrainian and Russian sources use different terms for rebels. Russian sources may call them 'militia' or 'guerilla' or 'insurgents.' Ukrainian sources will call them 'terrorists' or 'occupiers.'

- **INITIATOR: name of unit?** (see list)

If the report specifies the army service, unit, rebel group or volunteer 'battalion' carrying out the attack, enter it here.

The main units on the Ukrainian **government** side are:

- **ARMY:** Army
  - \* Air defense
  - \* Airmobile
  - \* Armored
  - \* Infantry
  - \* Rocket Forces
- **AF:** Air Force
- **AIRBORNE:** Airborne/Paratroopers
- **MARINE:** Marines
- **MVD:** Interior Ministry
- **NG:** National Guard
- **BG:** Border Guard
- **SBU:** State Security Services

- **VOLUNTEER:** Volunteer battalions

Note that many of the volunteer battalions are named after cities and regions, so double-check to make sure it's really a battalion. The more prominent battalions are marked with an asterisk (\*).

\* Aidar\*, Artemivsk, Azov\*, Batkivshchyna\*, Bogdan, Chernihiv, Dnipro/Dnepr\*, Donbas\*, Donetsk-1, Donetsk-2, Ivano-Frankivsk, Kharkiv-1, Kharkiv-2, Kherson, Kirovohrad, Kremenchuk, Kryvbas\*, Kyiv-1, Kyiv-2, Kyivshchyna, Kyivska Rus\*, Luhansk-1, Lviv, Maidan, Mariupol, Myrnyi, Myrotvorets, Poltava, Prykarpattia\*, Rukh Oporu\*, Shakhtar\*, Shakhtarsk, Shtorm, Sich, Sicheslav, Skif, Slobozhanshchyna, Sumy, Svityaz, Svyatyi Mykolai, Ternopil, Ukraine\*, Vinnytsia, Volyn\*, Volya\*, Zaporizhia, Zoloti Vorota

The main units on the **rebel** side are:

- **NOVROS:** Novorossiia Armed Forces
- **DNR:** Donetsk People's Republic (DNR)
- **LNR:** Lugansk People's Republic (LNR)
- **VOSTOK:** Vostok Battalion
- **OPLLOT:** Oplot
- **KALMUS:** Kal'mus battalion
- **BEZLER:** Bezler band
- **ZARYA:** Zarya battalion
- **RPA:** Russian Orthodox Army (RPA)
- **NOD:** People's Militia of Donbass (NOD)
- **PRIZRAK:** Prizrak battalion
- **AUV:** Army of the South East
- **COSSACK:** Don Cossacks
- **RNE:** Russian National Unity
- **ESM:** Eurasian Youth Union
- **YS:** Yovan Sevic
- **RUSSIA:** Russian Armed Forces

- **TARGET:** Government/rebel/unknown/civilian/other (G/R/U/C/O)

Enter G for government, R for rebel, U for unknown, C for civilian, O for other (e.g. Russian armed forces).

- **TARGET:** name of unit? (see list)

If the report specifies the army service, unit, rebel group or volunteer 'battalion' carrying out the attack, enter it here.

- **TYPE OF ACTION:** tactic or weapons system used

Below is a list of common categories:

- **AAD:** anti-air defense, Buk, shoulder-fired missiles (Igla, Strela)
- **AMBUSH:** surprise attack
- **AIRSTRIKE:** air strike, strategic bombing, helicopter strike
- **ARMOR:** tank battle or assault
- **ARREST:** arrest/detention
- **ARTILLERY:** shelling by field artillery, howitzer, mortar ('mine-thrower')
- **CONTROL:** establishment/claim of territorial control over population center

- **KILLING**: assassination, execution, extrajudicial killing, other targeted killing
- **KILLING\_A**: attempted (unsuccessful) assassination, execution, extrajudicial killing, other targeted killing
- **FIREFIGHT**: any exchange of gunfire with handguns, semi-automatic rifles, automatic rifles, machine guns, rocket-propelled grenades (RPGs)
- **IED**: improvised explosive device, roadside bomb, landmine, car bomb
- **PROPERTY**: property destruction
- **PROTEST**: non-violent protest
- **PROTEST\_V**: violent protest
- **RAID**: assault/attack, followed by a retreat
- **RIOT**: violent public disturbance against property or people
- **ROBBERY**: robbery, burglary, theft
- **ROCKET**: shelling by artillery rockets like Grad/BM-21, Uragan/BM-27, other Multiple Launch Rocket System (MRLS)
- **OCCUPY**: occupation of territory or building
- **STORM**: storming of a building or base
- **UNKNOWN**

- **CASUALTIES: civilians killed**

Number of reported civilian deaths.

- **CASUALTIES: civilians wounded**

Number of reported civilian wounded or injured.

- **CASUALTIES: rebels killed**

Number of reported rebel deaths.

- **CASUALTIES: rebels wounded**

Number of reported rebels wounded.

- **CASUALTIES: government killed**

Number of reported government/military deaths.

- **CASUALTIES: government wounded**

Number of reported government/military wounded.

- **Comments? (optional)**

Write any information you feel is relevant, but not captured by the questionnaire.

- **Do you want to re-enter your responses? (Y/N)**

Answer 'Y' (or 'y' or 'yes' or '1') if you made a mistake, or omitted something.

- **Additional events in record? (Y/N)**

Answer 'Y' (or 'y' or 'yes' or '1') if the report contains multiple events. You will then have a chance to enter info for additional events in the same report.

## 2.2 Intercoder reliability

To account for potential disagreement between coders, at least two sets of eyes read each training set document, including one of the authors and another member of the research team. Inter-coder reliability statistics, reported below, indicate a high and statistically significant level of agreement between coders on the relevant categories, including where coders read the same documents in different languages.

Table 2: INTERCODER RELIABILITY STATISTICS: REBEL VIOLENCE.

	Agree	Fleiss' Kappa	Kendall's W	Krippendorff's Alpha	N
<b>5.ua</b>	2 coders: both Ukrainian				
Violent event: 'Yes'	82.54	0.65***	0.84***	0.65 (0.51,0.78)	401
INITIATOR: 'Rebel'	84.79	0.6***	0.8***	0.59 (0.42,0.77)	401
<b>BFM (ru)</b>	3 coders: 1 Russian, 2 English				
Violent event: 'Yes'	80.69	0.45***	0.75***	0.46 (0.21,0.65)	606
INITIATOR: 'Rebel'	83.17	0.41***	0.72***	0.4 (0.17,0.62)	606
<b>Espreso.tv (ua)</b>	2 coders: both Ukrainian				
Violent event: 'Yes'	89.14	0.78***	0.9***	0.79 (0.66,0.9)	313
INITIATOR: 'Rebel'	85.94	0.62***	0.81***	0.6 (0.44,0.76)	313
<b>Gazeta.ru</b>	2 coders: 1 Russian, 1 English				
Violent event: 'Yes'	96.2	0.75***	0.87***	0.73 (0.45,0.94)	500
INITIATOR: 'Rebel'	87.34	0.61***	0.8***	0.61 (0.42,0.79)	500
<b>Interfax (ru)</b>	2 coders: 1 Russian, 1 English				
Violent event: 'Yes'	97.33	0.65***	0.83***	0.59 (0.22,0.96)	500
INITIATOR: 'Rebel'	88.67	0.39***	0.7***	0.4 (0.14,0.67)	500
<b>Interfax (ua)</b>	2 coders: 1 Russian, 1 English				
Violent event: 'Yes'	96.45	0.73***	0.87***	0.73 (0.38,0.93)	301
INITIATOR: 'Rebel'	88.07	0.58***	0.8***	0.57 (0.37,0.77)	301
<b>Lenta.ru</b>	3 coders: 1 Russian, 2 English				
Violent event: 'Yes'	94.94	0.69***	0.84***	0.63 (0.26,0.88)	500
INITIATOR: 'Rebel'	82.28	0.53***	0.77***	0.51 (0.34,0.69)	500
<b>OSCE (int)</b>	2 coders: both English				
Violent event: 'Yes'	93.08	0.77***	0.89***	0.77 (0.58,0.9)	300
INITIATOR: 'Rebel'	89.23	0.63***	0.82***	0.62 (0.43,0.81)	300
<b>Rusvesna.su</b>	2 coders: both Russian				
Violent event: 'Yes'	82.92	0.55***	0.79***	0.55 (0.38,0.74)	281
INITIATOR: 'Rebel'	80	0.51***	0.76***	0.5 (0.3,0.68)	281
<b>Sprotyv (ua)</b>	3 coders: 1 Russian, 2 English				
Violent event: 'Yes'	92.01	0.59***	0.81***	0.58 (0.33,0.83)	511
INITIATOR: 'Rebel'	96.49	0.65***	0.83***	0.65 (0.26,1)	511
<b>Ukrinform</b>	3 coders: 1 Russian, 2 English				
Violent event: 'Yes'	76.65	0.53***	0.77***	0.53 (0.38,0.68)	394
INITIATOR: 'Rebel'	86.67	0.56***	0.78***	0.56 (0.31,0.77)	394
<b>Wikipedia (ru)</b>	2 coders: both Russian				
Violent event: 'Yes'	91.54	0.64***	0.83***	0.63 (0.43,0.8)	130
INITIATOR: 'Rebel'	78.5	0.52***	0.76***	0.52 (0.32,0.7)	130

\* $p < .05$ , \*\* $p < .01$ , \*\*\* $p < .001$

### 2.3 Support vector machine

We used the randomly-selected reference texts in each training set to train a Support Vector Machine (SVM) classifier to predict the categories for all previously unseen corpus texts. The SVM classifies documents by fitting a maximally-separating hyperplane to a feature space, examining combinations of features that best yield separable categories. Formally, the SVM separates data points from each other according to their labels ( $y_{it} \in \{-1, 1\}$ ), and finds maximum marginal distance  $\Delta$  between the points labeled  $y_{it} = 1$  and  $y_{it} = -1$ , solving the optimization problem

$$\arg \max_{\Delta, \alpha, \phi} \Delta \text{ s.t. } y_{it}(\alpha + \phi(X_{it})) > \Delta$$

where  $y_{it}(\alpha + \phi(X_{it}))$  is a functional margin,  $\phi()$  is a function that maps the training data  $X$  to a high-dimensional space, and  $\mathbf{K}(x_i, x_j) = \phi(x_i)' \phi(x_j)$  is a kernel function. The advantage of the SVM is that it is well-suited to sparse, high-dimensional data, is highly robust, and can handle a low training-to-test data ratio.

We created a separate document-term matrix for each corpus, and ran the SVM classifier separately for each. In the document-term matrix, the rows are documents  $d \in \{1, \dots, D\}$ , columns are terms  $t \in \{1, \dots, T\}$ , cell entries are weighted term frequencies, and each row vector  $\mathbf{y}_d \in \mathbb{R}^T$  represents document  $d$  in a  $T$ -dimensional feature space. Features were weighted by term frequency - inverse document frequency,

$$tf.idf_{dt} = tf_{dt} \log \left( \frac{D}{df_t} \right)$$

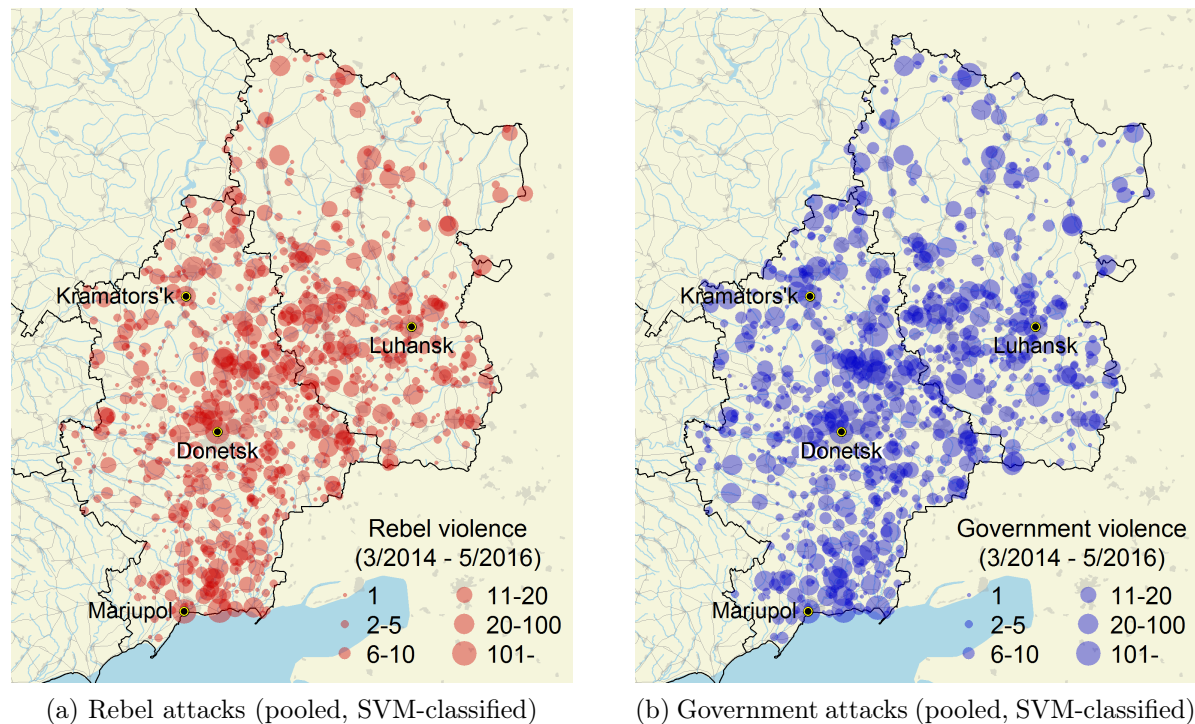
where  $tf_{dt}$  is term frequency (number of times term appears in  $d$ ), and  $df_t$  is document frequency (# documents with term  $t$ ). A high  $tf.idf_{dt}$  weight indicates that a term appears a lot in document  $d$ , but rarely in the corpus.

In the preprocessing stage, we removed HTML tags, control characters, non-alphanumeric characters, capitalization, punctuation and stopwords for all corpora, but ran a stemming algorithm only on English-language texts, so as to preserve inflections in Ukrainian and Russian (i.e. tense, voice, aspect, person, number, gender and case) – which contain important information for differentiating between initiators and targets.

To pool the data across the sources shown in Table 1, we used a one-a-day filter for each municipality-day. For each of 3,037 unique populated places in Donetsk, Luhansk oblasts, on each day between February 28, 2014 and February 29, 2016, we coded a rebel attack as occurring if at least one of the twelve SVM-classified datasets reported it as occurring. This technique, common in event data research, is designed to eliminate double-counts.

This filter produced 26, 289 unique violent events. We aggregated these individual records into event counts in daily and weekly time series. Because the one-a-day filter implies a maximum of one event per municipality on a given day, the daily intensities of rebel and government violence can be interpreted as the number of municipalities experiencing violence by each actor per day. The range of these variables is 0 (no municipalities in violence) to 3,037 (all Donbas municipalities experiencing violence). Figure 1 visualizes the overall intensity of violence across the 3,037 populated places of the Donbas for the full study period.

Figure 1: GEOGRAPHIC DISTRIBUTION OF KINETIC OPERATIONS



### 3 Holidays and other political events (Ukraine)

To account for increases in digital attacks during holiday periods, we control for Ukrainian, Russian and Soviet holidays. The Ukrainian Cyber Forces, for instance, conducted an operation called “Happy New Year,” whose aim was to hack into printers in the Crimea, Russia, and Donbas to print pro-Ukrainian messages.

Figure 2 displays cyber attacks in eastern Ukraine during the period of August 2013 to February 2016. In this figure, Cyber U indicates operations by pro-Ukrainian government forces and Cyber R captures operations by pro-Russian rebel groups. There is a spike of pro-Ukrainian cyber operations during the period of winter holidays in Ukraine, from December 31st to January 19th. The opposite trend is evident in Figure 3, where physical violence declined during the holiday season in Ukraine.

In addition to holidays common to all sides (i.e. New Year’s Day, Christmas, Easter), Ukrainian holidays include May 8 (Victory Day), June 28 (Constitution Day), August 24 (Independence Day), October 14 (Defender of Ukraine Day) and November 21 (Anniversary of Euromaidan). Russian holidays include February 23 (Defender of the Fatherland Day), May 9 (Victory Day), June 12 (Russia Day) and November 4 (Unity Day). Soviet holidays include February 23 (Red Army Day), March 8 (Women’s Day), May 1 (Labor Day), May 9 (Victory Day), November 7 (Revolution Day).

The parliamentary and presidential electoral campaigns are another time when activities on the online front have increased. Specifically, a few days before and during the presidential campaigns, the Central Electoral Committee’s website was bombarded with DDoS attacks. Figure 2 displays an increase of pro-Russian operations ahead of the presidential elections on May 25, 2014.

Finally, we control for variation in kinetic and cyber operations during periods of ceasefire



following the ‘Minsk I’ and ‘Minsk II’ agreements. For example, the intensity of the cyber espionage operation “Armageddon” – often claimed to be Russia-sponsored and aimed at hacking the websites of Ukrainian government agencies – increased right before the ‘Minsk I’ (September 5, 2014) and ‘Minsk II’ (February 12, 2015) agreements; however, its activity rapidly declined after the ceasefires. Similarly, the intensity of the kinetic operations of both sides has decreased to some extent right after the agreements.

Figure 2: CYBER ATTACKS IN EASTERN UKRAINE. (August 2013 – February 2016)

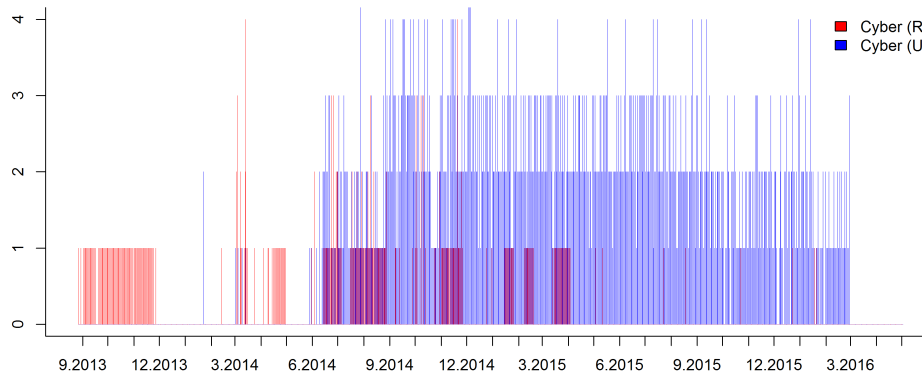
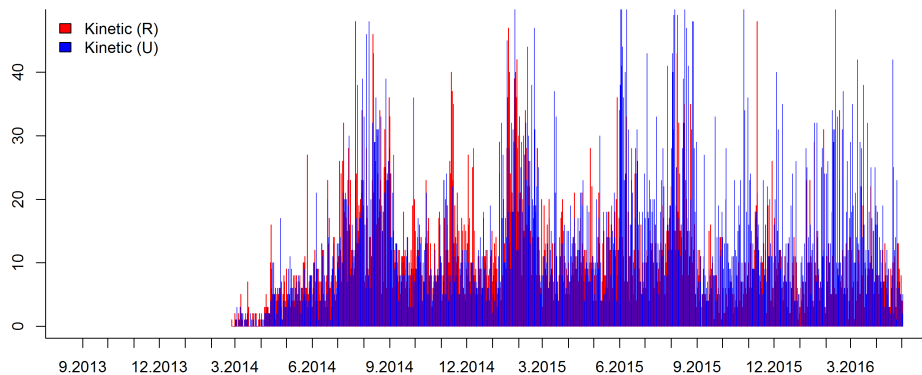


Figure 3: KINETIC ATTACKS IN EASTERN UKRAINE. (March 2014 – February 2016)



## 4 Variable descriptions for aggregated data (Ukraine)

Blue variable names indicate presence in daily data only. Red variable names indicate presence in weekly data only.

### 4.1 Geographic locations and dates

**Time ID (DAY) (TID)** Unique identifier for each day.

**Time ID (week) (WID)** Unique identifier for each week.

**Year (YEAR)** Year of observation.

**Month (MONTH)** Month of observation.

**District Name (GADM\_NAME\_2)** Name of district/raion.

## 4.2 Kinetic operations

**Ukrainian kinetic operations (count) (GOV\_ALL, GOV\_ALL\_b)** total number of episodes of pro-Ukrainian violence of any type, observed on day (week)  $t$

**Pro-Russian rebel kinetic operations (count) (REB\_ALL, REB\_ALL\_b)** total number of episodes of rebel violence of any type, observed on day (week)  $t$

## 4.3 Cyber operations

**Ukrainian cyber operations (count) (CYBER\_UA)** total number of cyber attacks by pro-Ukrainian groups, observed on day (week)  $t$

**Pro-Russian rebel cyber operations (count) (CYBER\_RUREB)** total number of cyber attacks by pro-rebel groups, observed on day (week)  $t$

## 4.4 Explanatory variables

**2014 Ukrainian presidential elections (ELECTIONS\_UPR2014)**  $\begin{cases} 1 & \text{if } 2/25/2014 \leq t \leq 5/25/2014 \\ 0 & \text{otherwise} \end{cases}$

**2014 Ukrainian parliamentary elections (ELECTIONS\_UPL2014)**  $\begin{cases} 1 & \text{or } 8/28/2014 \leq t \leq 10/26/2014 \\ 0 & \text{otherwise} \end{cases}$

**Any 2014 Ukrainian elections (ELECTIONS\_U2014)**  $\begin{cases} 1 & \text{if } 2/25/2014 \leq t \leq 5/25/2014 \\ & \text{or } 8/28/2014 \leq t \leq 10/26/2014 \\ 0 & \text{otherwise} \end{cases}$

**2014 DNR/LNR elections (ELECTIONS\_D2014)**  $\begin{cases} 1 & \text{if } 9/23/2014 \leq t \leq 11/2/2014 \\ 0 & \text{otherwise} \end{cases}$

**Ukrainian holidays (HOLIDAYS\_UKR)**  $\begin{cases} 1 & \text{if } t \in \{5/8, 6/28, 8/24, 10/14, 11/21\} \\ 0 & \text{otherwise} \end{cases}$

**Russian holidays (HOLIDAYS\_RUS)**  $\begin{cases} 1 & \text{if } t \in \{2/23, 5/9, 6/12, 11/4\} \\ 0 & \text{otherwise} \end{cases}$

**Soviet holidays (HOLIDAYS\_SOV)**  $\begin{cases} 1 & \text{if } t \in \{1/1, 2/23, 3/8, 5/1, 5/9, 11/7\} \\ 0 & \text{otherwise} \end{cases}$

**Minsk I ceasefire (MINSK1)**  $\begin{cases} 1 & \text{if } 9/5/2014 \leq t \leq 2/14/2015 \\ 0 & \text{otherwise} \end{cases}$

$$\text{Minsk II ceasefire (MINSK2)} \begin{cases} 1 & \text{if } t \geq 2/15/2015 \\ 0 & \text{otherwise} \end{cases}$$

## 5 Summary statistics (Ukraine)

Figure 4: CORRELATION BETWEEN EXPLANATORY VARIABLES.



Table 3: SUMMARY STATISTICS FOR THE UKRAINE DATA

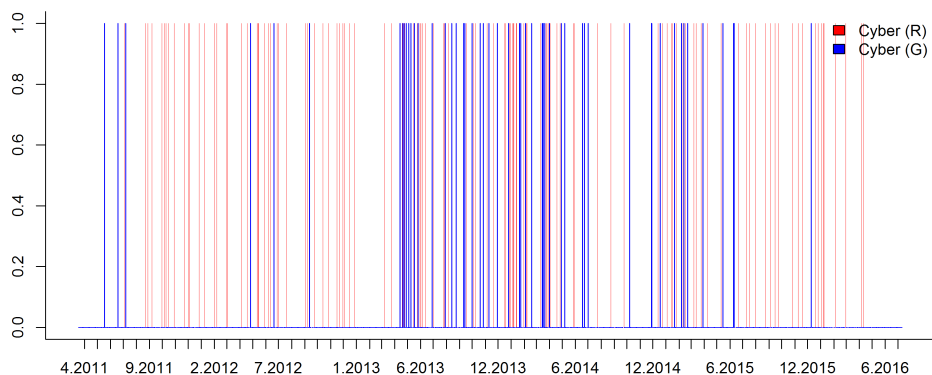
	Obs	Mean	Median	SD	Min	Max
<i>Outcome variables</i>						
Ukrainian (pro-government) kinetic operations	980	14.04	11.00	10.97	0.00	68.00
Rebel (pro-Russia) kinetic operations	980	11.27	9.00	8.13	0.00	48.00
Ukrainian (pro-government) cyber	980	1.04	0.00	1.81	0.00	6.00
Rebel (pro-Russia) cyber	980	0.32	0.00	0.70	0.00	7.00
<i>Covariates</i>						
2014 Ukrainian Presidential elections	980	0.09	0.00	0.28	0.00	1.00
2014 Ukrainian Parliamentary elections	980	0.06	0.00	0.23	0.00	1.00
2014 Ukrainian elections	980	0.15	0.00	0.36	0.00	1.00
2014 Donetsk elections	980	0.04	0.00	0.20	0.00	1.00
Ukrainian holidays	980	0.01	0.00	0.11	0.00	1.00
Russian holidays	980	0.01	0.00	0.10	0.00	1.00
Soviet holidays	980	0.02	0.00	0.13	0.00	1.00
'Minsk 1' agreement	980	0.17	0.00	0.37	0.00	1.00
'Minsk 2' agreement	980	0.45	0.00	0.50	0.00	1.00

## 6 Cyber operations data (Syria)

Our cyber operations data for Syria comprise 682 attacks, ranging from May 2011 until June 2016. Data sources 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). As evident from Figure 5, Syrian cyber operations are much sparser than the Ukrainian ones.

Figure 5: CYBER ATTACKS IN SYRIA FROM MARCH 2011 TO JUNE 2016.



## 6.1 Classification and description of cyber operations data

After cross-checking all cyber events with multiple sources, we classified them using this codebook:

### Syria Cyber Attacks Codebook

1. ATTACK\_ID
2. DATE (YYYYMMDD format)
3. INITIATOR (partisanship) - whether the group is pro-Assad, pro-West, or supports any other actor in the conflict.
  - (a) **1 - anti-Assad** – The various international governmental units and officials, private businesses, non-state militias, and individuals that denounce the Assad government in Syria. These groups are not complete supporters of Western intervention, and yet often attack Western units to promote Anti-Assad propaganda. This group also includes supporters of the Islamic State of Iraq and Syria's ideals who reject and engage in cyber-attacks against the Assad government as well as other Middle Eastern and Western governments and private individuals.
  - (b) **2 - Pro-Assad** – International governmental units and officials, Syrian government-sponsored units, and private citizens that support and defend the current Assad government in Syria.
4. INITIATOR\_UNIT - name of the group that executes attacks (e.g., *Syrian Electronic Army*)
  - (a) Anti-Assad
    - i. ANO – attacks either executed by *Anonymous* or by *Anonymous* - sponsored units (e.g., non-state actors participating in #OpIstis operation)
    - ii. AAN -Anti-Assad non-state actors (e.g., private citizens etc.)
    - iii. JSU - Jabhat al-Nusra-sponsored units

- iv. KSO - Kurdish non-state opposition
- v. PSN - Pro-Islam non-state units
- (b) Pro-Assad
  - i. ISU -ISIL/ISIS units
  - ii. ISS - ISIL/ISIS - sponsored units (e.g., *Lizard Squad*, *Cyber Caliphate*)
  - iii. RGU - Russian government units
  - iv. SSU- Syrian state-sponsored units (e.g., *Syrian Electronic Army (SEA)*, *Syrian Malware Team*)
  - v. SGU - Syrian government units
- 5. INITIATOR\_STATE
  - (a) 1 - State Actor;
  - (b) 0 - Non-state Actor;
- 6. DISPUTED
  - (a) 1 - Disputed. In the case when no one claimed responsibility for their actions, such attacks were marked as “disputed.”
  - (b) 0 - Non-disputed. Cyber attacks for which non-state actors claimed responsibility on their social media platforms or in interviews with mass media representatives are labeled “non-disputed.”
- 7. TARGET (partisanship)
  - (a) 1 - Anti-Assad
  - (b) 2 - Pro-Assad
- 8. TARGET\_UNIT\_1 - name of the target
  - (a) Anti-Assad
    - i. AAN - Anti-Assad non-state actors (e.g., private citizens) (e.g., *Cyber Justice Team*). This subcategory does not include attacks by the militia group *Free Syrian Army*.
    - ii. FSA - *Free Syrian Army*, a prominent militia of defected officers from the Syrian Armed Forces that pledge to overthrow the Assad government. One of the only militias engaged in cyber operations as well as a ground conflict against the Assad government.
  - (b) Pro-Assad
    - i. PAN - Pro-Assad non-state actors (e.g., mass media, private companies and citizens, etc.)
    - ii. PIS - Pro-ISIL social media and websites
    - iii. SSU- Syrian state-sponsored units (e.g., *Syrian Electronic Army (SEA)*, *Syrian Malware Team*)
    - iv. SGU - Syrian government units
    - v. SGO - Syrian government officials
- 9. TARGET\_UNIT\_2
- 10. TAGRGET\_STATE\_1 - whether the target is a state or non-state actor
  - (a) 1 - State Actor;
  - (b) 0 - Non-state Actor;
- 11. TARGET\_STATE\_2
- 12. ATTACK\_TYPE\_1 - cyber techniques used in cyber operations.
  - (a) AVG - collecting audio-, video-, and geo-intelligence; it could be done via hacking into CCTV cameras, listening to conversations, etc;
  - (b) BWC - blocking websites via sending/filing complaints to the companies that host those websites;
  - (c) CPI - collecting private information via open sources;

- (d) DDS - distributed denial-of-service attack, including TCP SYN floods. It is a “type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. A Denial of Service (DoS) attack is different from a DDoS attack. The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.”<sup>9</sup>
- (e) ODS - other individual attacks with a purpose of disruption or espionage. This category includes usage of malware (software that is intended to damage or disable computers and computer systems) or a malicious code. We combine these attacks into one category because of their low frequency in our data set;
- (f) PPI - publishing online private information of the members of the conflicting parties (e.g. bank account info, DOB, identification codes, addresses, etc);
- (g) SPE - spear-phishing email (an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data). This category also includes phishing emails (the activity of defrauding an online account holder of financial information by posing as a legitimate company);
- (h) STM - sending massive text messages or calling phones non-stop;
- (i) UNK - unknown, not specified;
- (j) WBG - website blockage is “a process by which a Firewall or WWW Proxy prevents users from accessing some network resources, such as World-Wide Web sites or Ftp servers.”<sup>10</sup> This category also includes blocking websites via sending/filing complaints to the companies that host those websites;
- (k) WDT - website defacement “is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.”<sup>11</sup> This category also include defacement of social media accounts;

## 13. ATTACK\_TYPE\_2

## 14. ATTACK\_GOAL - a purpose of the attack

- (a) PRP - mainly propaganda with a purpose of either to influence public opinion or to hurt financing or recruitment campaigns;
- (b) DSR - disruption, espionage, sabotage, using cyber means;
- (c) BTH - both (propaganda & disruption)

## 15. OPERATION\_NAME

- (a) ISS - social media accounts of ISIS/ISIL or ISIL/ISIS - sponsored units (e.g., *Lizard Squad*, *Cyber Caliphate*)
- (b) OIS - #OpISIS;
- (c) OPS - #OpSyria;
- (d) OSU - #OpISU, operation by the *Anonymous*-sponsored units;
- (e) OTH - other; these group includes individual operations that do not repeat in our data more than three times;
- (f) UKN - non-provided;

## 16. REPORTING\_SOURCE\_1

- (a) ASU - social media accounts of *Anonymous* or *Anonymous*- supported groups (e.g., *New World Hacking*)
- (b) CNS - computer-security news sources, including *Graham Cluley*, *TechWeek Europe*, *Arstechnica*, *Information Week*, *Digital Dao*, *Computer Weekly*, *Tech News*, *Wired*, *Security Affairs*;
- (c) MEM - Middle Eastern mass media sources (e.g., *Turkish News*, *Arabiya*, *Doha News*, etc.)
- (d) OTH - other, social media individual accounts, mostly Twitter accounts;
- (e) RMM - Russian mass media and social media (e.g., *RT.com*, *Yahoo.com*)
- (f) SEA - *Syrian Electronic Army*'s social media accounts;
- (g) TCM - tech companies (e.g., *Risk Based Security*, *Electronic Frontier Foundation*, etc)
- (h) WNS - 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.);
- (i) YTB - Youtube;
- (j) ZHO - zone-h.org website

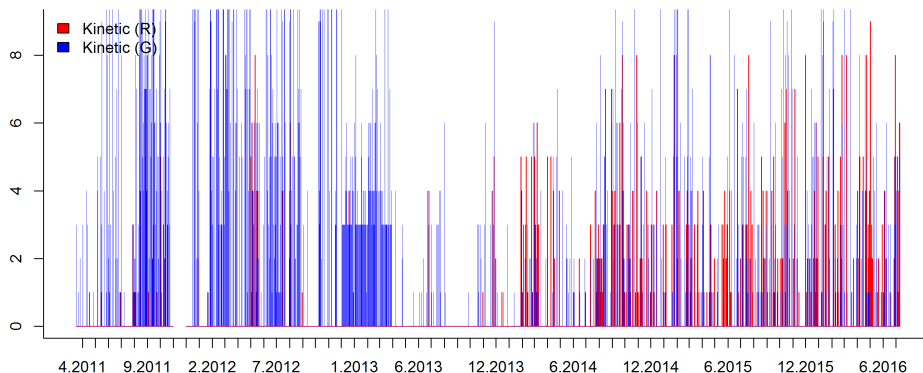
## 17. REPORTING\_SOURCE\_2

## 18. REPORTING\_SOURCE\_3

## 7 Violent events data (Syria)

Our data on kinetic operations rely on human-assisted machine coding of event reports from the IISS Armed Conflict Database. Because the event classification method (Support Vector Machine) was identical to that used for violent events in Ukraine, we omit technical details here to avoid repetition. Training set codebook is available on request.

Figure 6: KINETIC ATTACKS IN SYRIA FROM MARCH 2011 TO JUNE 2016



## 8 Variable descriptions for aggregated data (Syria)

Blue variable names indicate presence in daily data only. Red variable names indicate presence in weekly data only.

### 8.0.1 Geographic locations and dates

**Time ID (DAY) (TID)** Unique identifier for each day.

**Time ID (week) (WID)** Unique identifier for each week.

**Year (YEAR)** Year of observation.

**Month (MONTH)** Month of observation.

### 8.0.2 Kinetic operations

**Syrian kinetic operations (count) (GOV\_ALL, GOV\_ALL\_b)** total number of episodes of pro-Assad violence of any type, observed on day (week)  $t$

**Pro-rebel kinetic operations (count) (REB\_ALL, REB\_ALL\_b)** total number of episodes of rebel violence of any type, observed on day (week)  $t$

### 8.0.3 Cyber operations

**Pro-Assad cyber operations (count) (CYBER\_PAS)** total number of cyber attacks by pro-Assad groups, observed on day (week)  $t$

**Anti-Assad rebel cyber operations (count) (CYBER\_AAS\_COMB)** total number of cyber attacks by pro-rebel groups, observed on day (week)  $t$

#### 8.0.4 Explanatory variables

**2014 Syrian presidential elections (ELECTIONS\_SPR2014)**  $\begin{cases} 1 & \text{if } 4/8/2014 \leq t \leq 6/3/2014 \\ 0 & \text{otherwise} \end{cases}$

**2012 Syrian parliamentary elections (ELECTIONS\_SPL2012)**  $\begin{cases} 1 & \text{if } 3/13/2012 \leq t \leq 5/7/2012 \\ 0 & \text{otherwise} \end{cases}$

**2016 Syrian parliamentary elections (ELECTIONS\_SPL2016)**  $\begin{cases} 1 & \text{if } 2/22/2016 \leq t \leq 4/13/2016 \\ 0 & \text{otherwise} \end{cases}$

**Any Syrian elections (ELECTIONS\_SYRIA)**  $\begin{cases} 1 & \text{if } 3/13/2012 \leq t \leq 5/7/2012 \\ & \text{or } 4/8/2014 \leq t \leq 6/3/2014 \\ & \text{or } 2/22/2016 \leq t \leq 4/13/2016 \\ 0 & \text{otherwise} \end{cases}$

**2012 Syrian referendum (REFERENDUM\_S2012)**  $\begin{cases} 1 & \text{if } 2/26/2012 \leq t \leq 2/26/2012 \\ 0 & \text{otherwise} \end{cases}$

**Syrian holidays (HOLIDAYS\_SYR)**  $\begin{cases} 1 & \text{if } t \in \{03/08, 04/17, 05/01, 05/06, 08/01, 10/06\} \\ 0 & \text{otherwise} \end{cases}$

**Islamic holidays (HOLIDAYS\_MUS)**  $\begin{cases} 1 & \text{if } t \in \{02/15/11, 08/01/11, 08/02/11 - 08/30/11, 11/06/11, \\ & 11/26/11, 02/04/12, 07/20/12-08/19/12, 10/26/12, 11/15/12, \\ & 01/23/13, 07/09/13-08/08/13, 11/05/13, 01/13/14, \\ & 06/28/14-07/28/14, 10/04/14, 10/25/14, 01/03/15, \\ & 06/18/15-07/17/15, 10/15/13, 09/23/15, 10/24/15, \\ & 06/06/16-07/05/16 \\ 0 & \text{otherwise} \end{cases}$

**‘Annan’ 2012 ceasefire (ANNAN2012)**  $\begin{cases} 1 & \text{if } 4/12/2012 \leq t \leq 10/26/2012 \\ 0 & \text{otherwise} \end{cases}$

**‘Eid’ 2012 ceasefire (EID2012)**  $\begin{cases} 1 & \text{if } t \geq 10/26/2012 \\ 0 & \text{otherwise} \end{cases}$

**‘Munich’ 2016 ceasefire (MUNICH2016)**  $\begin{cases} 1 & \text{if } t \geq 2/27/2016 \\ 0 & \text{otherwise} \end{cases}$

## 9 Holidays and other political events (Syria)

Similarly to the Ukrainian study, we control for holidays (Syrian and Islamic), Syrian presidential and parliamentary elections, and the 2012 referendum. Additionally, we control for variation in kinetic and cyber operations during periods following ceasefire agreements in 2012 and 2016.



Figure 7: CORRELATION BETWEEN EXPLANATORY VARIABLES. SYRIA.

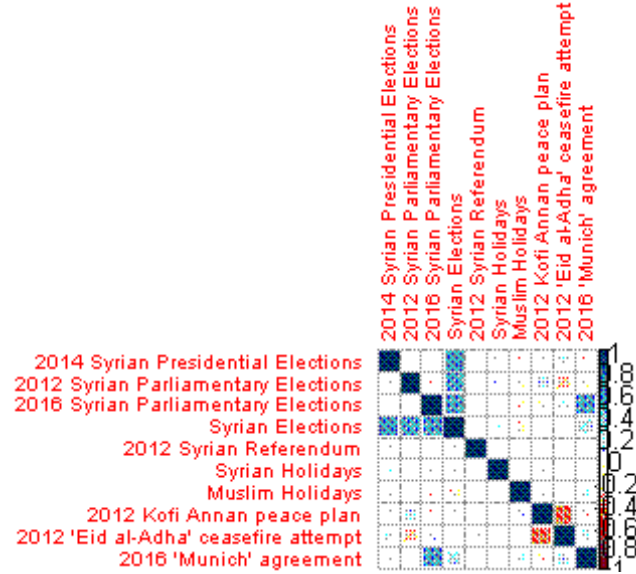


Table 4: SUMMARY STATISTICS FOR THE SYRIA DATA

	Obs	Mean	Median	SD	Min	Max
<i>Outcome variables</i>						
Syrian (pro-government) kinetic operations	1943	1.80	0.00	3.21	0.00	22.00
Rebel (anti-Assad) kinetic operations	1943	0.37	0.00	1.26	0.00	9.00
Pro-Assad cyber operations	1943	0.04	0.00	0.17	0.00	1.00
Anti-Assad cyber operations	1943	0.06	0.00	0.24	0.00	1.00
<i>Covariates</i>						
2014 Syrian Presidential elections	1943	0.03	0.00	0.17	0.00	1.00
2012 Syrian Parliamentary elections	1943	0.03	0.00	0.17	0.00	1.00
2016 Syrian Parliamentary elections	1943	0.03	0.00	0.16	0.00	1.00
Syrian Elections	1943	0.08	0.00	0.29	0.00	1.00
2012 Syrian Referendum	1943	0.00	0.00	0.02	0.00	1.00
Syrian holidays	1943	0.02	0.00	0.13	0.00	1.00
Muslim holidays	1943	0.10	0.00	0.30	0.00	1.00
2012 Kofi Annan peace plan	1943	0.10	0.00	0.30	0.00	1.00
2012 'Eid al-Adha' ceasefire attempt	1943	0.70	1.00	0.46	0.00	1.00
2016 'Munich' agreement	1943	0.45	0.00	0.25	0.00	1.00

## 10 Robustness checks

In addition to the results presented in the main text, we ran 8 sets of robustness checks, which we summarize in Tables 5– 6 below, and provide detailed results on subsequent pages.

Table 5: ROBUSTNESS CHECKS TESTS  
 IMPULSE RESPONSE FUNCTIONS (IRF), GRANGER CAUSALITY TEST (GCT) & VARIANCE DECOMPOSITION (VD)

Kinetic data (3/22/14-2/29/16) & Cyber data (8/27/13-2/29/16)							
ID	Cyber	IRF(d)	IRF(w)	GCT (d)	GCT (w)	VD (d) (results provided by a 30-day point)	VD(w) (results provided by a 12-week point)
1	All	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	2 weeks after 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)	shocks in Kin(R) account for 3% of variation in Kin(U), & Kin(U) → 17% of Kin(R)	shocks in Kin(R) account for 8% of variation in Kin(U), & Kin(U) → 45% of Kin(R); Kin(U) → 3% of Cyb(R)
2	Propaganda	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	2 weeks after Kin(R) → Kin(U); Kin(U) → Kin(R); 2 weeks after 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)	shocks in Kin(R) account for 3% of variation in Kin(U) & Kin(U) → 18% of Kin(R)	shocks in Kin(R) account for 9% of variation in Kin(U) & 3% of Cyb(R); Kin(U) → 46% of Kin(R), 5% of Cyb(U), & 2% of Cyb(R)
3	Disruption	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	2 weeks after Kin(R) → Kin(U); Kin(U) → Kin(R)	Kin(R) ↔ Kin(U); Cyb(U) ↔ Kin(U) & Kin(R)	Kin(R) → Kin(Cyb(U))	shocks in Kin(R) account for 3% of variation in Kin(U) & Kin(U) → 17% of Kin(R)	shocks in Kin(R) account for 8% of variation in Kin(U); Kin(U) → 45% of Kin(R)
4	Disruption & both	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	2 weeks after 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)	shocks in Kin(R) account for 3% of variation in Kin(U) & Kin(U) → 17% of Kin(R)	shocks in Kin(R) account for 8% of variation in Kin(U); Kin(U) → 45% of Kin(R)
Kinetic & Cyber data (5/11/14-2/11/15)							
5	All	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	Kin(U) → Kin(R)	Kin(R) ↔ Kin(U)		shocks in Kin(R) account for 7% of variation in Kin(U) & Kin(U) → 13% of Kin(R)	shocks in Kin(R) account for 2% of variation in Cyb(U) & 18% of Cyb(R); Kin(U) → 30% of Kin(R), 2% of Cyb(U), & 2% of Cyb(R); Cyb(U) → 4% of Kin(R); Cyb(R) → 3% of Kin(U)
6	Propaganda	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	2 weeks after Cyb(R) → Kin(U); Kin(U) → Kin(R)	Kin(R) ↔ Kin(U)	Kin(R) → Cyb(R)	shocks in Kin(R) account for 7% of variation in Kin(U) & Kin(U) → 13% of Kin(R)	shocks in Kin(U) → 27% of Kin(R) & 4% of Cyb(U); Kin(R) → 5% of Cyb(U) & 3% of Cyb(R); Cyb(U) → 9% of Kin(U), 2% of Kin(R) & 20% of Cyb(R); Cyb(R) → 5% of Kin(U) & 2% of Cyb(U)
7	Disruption	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	Kin(U) → Kin(R)	Kin(R) ↔ Kin(U)	Kin(U) → Cyb(U)	shocks in Kin(R) account for 7% of variation in Kin(U) & for 2% of variation in Cyb(R); Kin(U) → 12% of Kin(R); Cyb(R) → 2% of Kin(U)	shocks in Kin(U) → 29% of Kin(R), 34% of Cyb(U), & 22% of Cyb(R); Kin(R) → 3% of Kin(U), 10% of Cyb(U), & 13% of Cyb(R); Cyb(U) → 2% of Kin(U) & 6% of Cyb(R); Cyb(R) → 3% of Kin(R) & 7% of Cyb(U)
8	Disruption & both	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	Kin(U) → Kin(R)	Kin(R) ↔ Kin(U)		shocks in Kin(R) account for 7% of variation in Kin(U) & 2% of Cyb(R); Kin(U) → 12% of Kin(R) & for 2% of Cyb(R)	shocks in Kin(R) account for 10% of variation in Cyb(R); Kin(U) → 21% of Kin(R) & for 17% of Cyb(R); Cyb(U) → 4% of Cyb(R)
Syria data (3/17/2011-7/10/2016)							
9	Disruption & both	Kin(G) → Kin(R)	HAVE NOT RUN THE TEST	Kin(R) ↔ Kin(U)	HAVE NOT RUN THE TEST	shocks in Kin(u) account for 2% of variation in Kin(R)	HAVE NOT RUN THE TEST

Table 6: ROBUSTNESS CHECKS TESTS  
 MAIN RESULTS (5/11/14-2/15/15)

Impulse-response plots				
$IRF(d)$	$IRF(w)$	$IRF(o)(d)$	$IRF(o)(w)$	$IRF(d) Sources (RU)$
2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	Kin(U) → Kin(R)	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)	2 weeks after Kin(U) → Kin(R); Kin(R) → Kin(U)	2 days after Kin(R) → Kin(U); Kin(U) → Kin(R)
Gauger causality & Variance Decomposition tests				
$IRF(d) Sources (U)$	$GCT(d)$	$GCT(w)$	$VD(d)$ (results provided by a 30-day point)	$VD(w)$ (results provided by a 12-week point)
Kin(U) → Kin(G)	Kin(R) ↔ Kin(U)		shocks in Kin(R) account for 7% of variation in Kin(U) & 2% of variation in Cyb(R); shocks in Kin(U) account for 12% of variation in Kin(R) & for 2% of variation in Cyb(R)	shocks in Kin(R) account for 10% of variation in Cyb(R); shocks in Kin(U) account for 21% of variation in Kin(R) & for 17% of variation in Cyb(R); shocks in Cyb(U) account for 4% of variation in Cyb(R)

### 10.1 Test 1: All cyber and kinetic operations in Ukraine from August 17, 2013 to February 29, 2016

Figure 8: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 1**. 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.

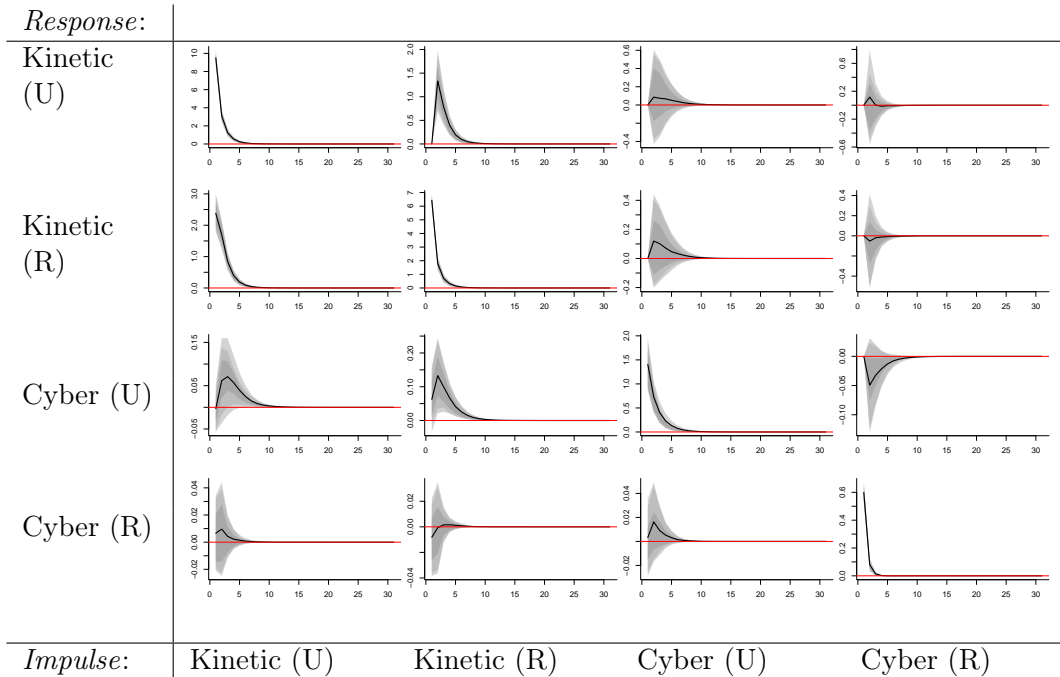


Figure 9: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 1**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

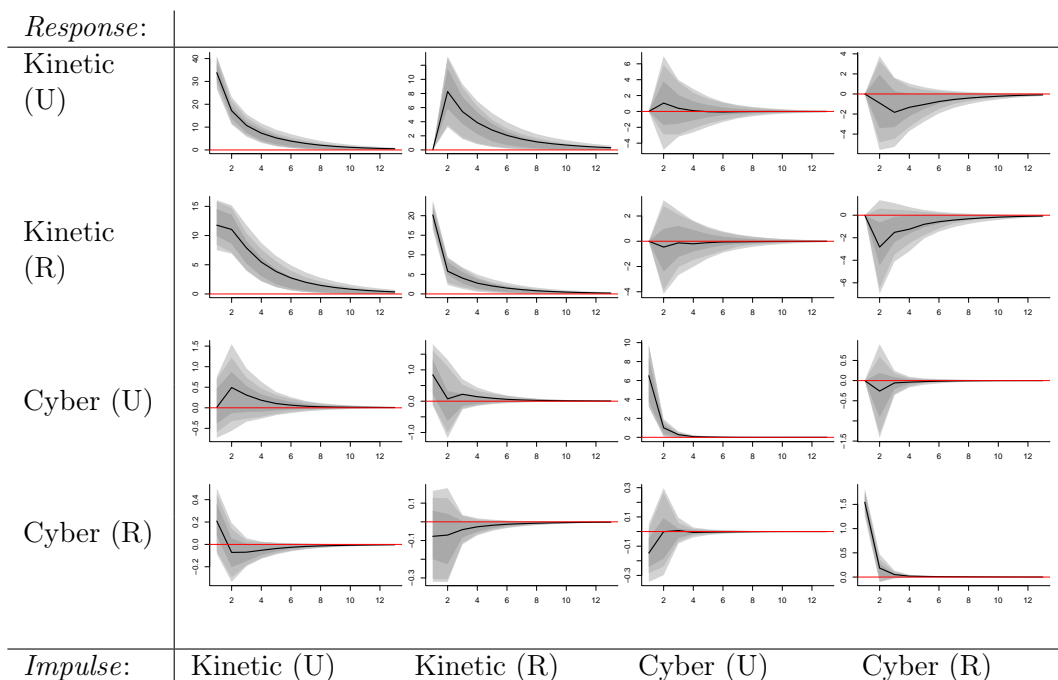


Table 7: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 1**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	20.85	0.00
Cyber (U) → Kinetic (U)	3.72	0.05
Cyber (R) → Kinetic (U)	4.91	0.03
Kinetic (U) → Kinetic (R)	15.99	0.00
Cyber (U) → Kinetic (R)	5.91	0.02
Cyber (R) → Kinetic (R)	0.59	0.44
Kinetic (U) → Cyber (U)	5.33	0.02
Kinetic (R) → Cyber (U)	14.70	0.00
Cyber (R) → Cyber (U)	3.09	0.08
Kinetic (U) → Cyber (R)	5.58	0.02
Kinetic (R) → Cyber (R)	0.70	0.40
Cyber (U) → Cyber (R)	2.00	0.16

Table 8: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 1.** ‘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)	8.61	0.00
Cyber (U) → Kinetic (U)	1.91	0.17
Cyber (R) → Kinetic (U)	1.56	0.21
Kinetic (U) → Kinetic (R)	1.49	0.23
Cyber (U) → Kinetic (R)	1.01	0.32
Cyber (R) → Kinetic (R)	0.06	0.81
Kinetic (U) → Cyber (U)	1.55	0.22
Kinetic (R) → Cyber (U)	3.85	0.05
Cyber (R) → Cyber (U)	1.07	0.30
Kinetic (U) → Cyber (R)	8.94	0.00
Kinetic (R) → Cyber (R)	2.13	0.15
Cyber (U) → Cyber (R)	1.60	0.21

Table 9: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 1.** ‘U’ indicates reported 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	0.982	0.018	0.000	0.000
7 days	0.974	0.026	0.000	0.000
30 days	0.974	0.026	0.000	0.000
Kinetic (R)				
1 day	0.119	0.881	0.000	0.000
2 days	0.161	0.839	0.000	0.000
7 days	0.174	0.825	0.000	0.000
30 days	0.174	0.825	0.000	0.000
Cyber (U)				
1 day	0.000	0.002	0.998	0.000
2 days	0.002	0.009	0.989	0.001
7 days	0.005	0.015	0.980	0.001
30 days	0.005	0.015	0.980	0.001
Cyber (R)				
1 day	0.000	0.000	0.000	1.000
2 days	0.000	0.000	0.000	0.999
7 days	0.000	0.000	0.001	0.999
30 days	0.000	0.000	0.001	0.999

Table 10: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 1.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.951	0.048	0.000	0.001
6 weeks	0.914	0.082	0.000	0.004
12 weeks	0.912	0.083	0.000	0.004
Kinetic (R)				
1 week	0.252	0.748	0.000	0.000
2 weeks	0.371	0.620	0.000	0.009
6 weeks	0.445	0.542	0.002	0.012
12 weeks	0.449	0.538	0.002	0.012
Cyber (U)				
1 week	0.001	0.013	0.986	0.000
2 weeks	0.004	0.013	0.981	0.002
6 weeks	0.006	0.013	0.979	0.002
12 weeks	0.006	0.013	0.979	0.002
Cyber (R)				
1 week	0.022	0.002	0.006	0.971
2 weeks	0.021	0.006	0.006	0.966
6 weeks	0.025	0.008	0.006	0.961
12 weeks	0.025	0.008	0.006	0.960

## 10.2 Test 2: ‘Propaganda’ cyber operations and physical violence in Ukraine from August 17, 2013 to February 29, 2016

Figure 10: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 2**. 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.

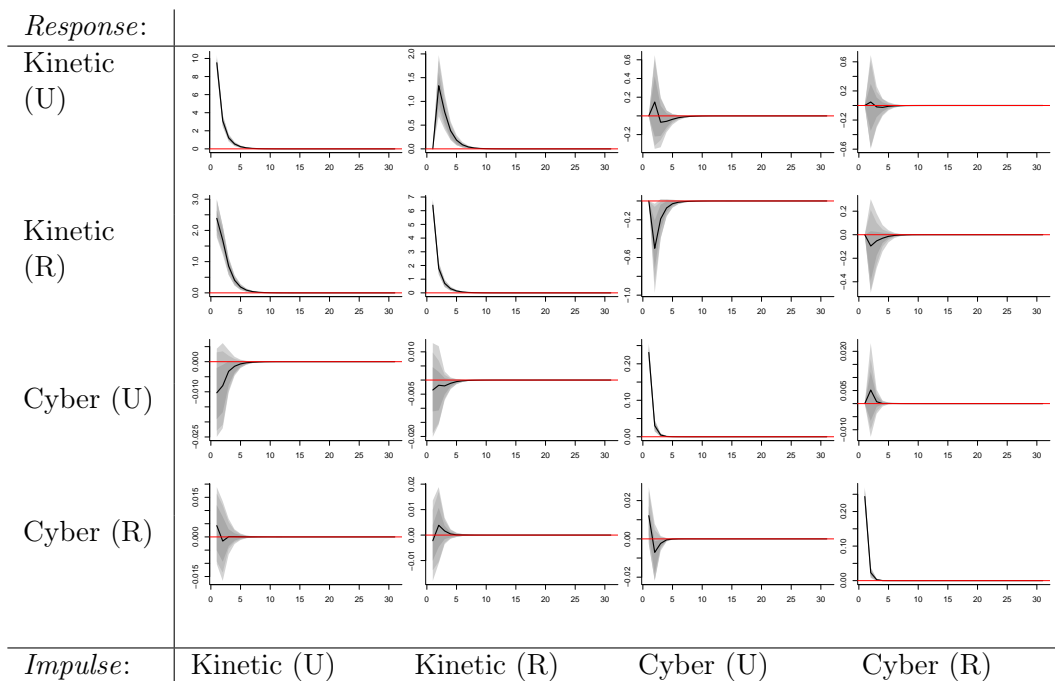


Figure 11: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 2**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

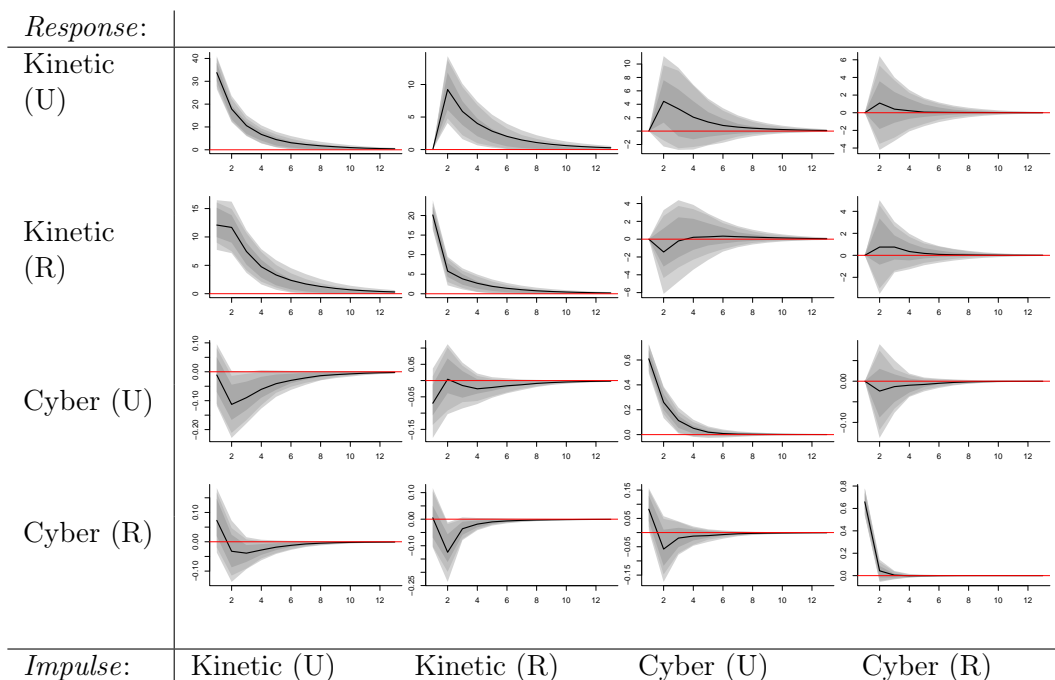


Table 11: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 2**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	20.85	0.00
Cyber (U) → Kinetic (U)	0.73	0.39
Cyber (R) → Kinetic (U)	1.72	0.19
Kinetic (U) → Kinetic (R)	15.99	0.00
Cyber (U) → Kinetic (R)	5.71	0.02
Cyber (R) → Kinetic (R)	0.90	0.34
Kinetic (U) → Cyber (U)	0.00	0.97
Kinetic (R) → Cyber (U)	1.94	0.16
Cyber (R) → Cyber (U)	0.65	0.42
Kinetic (U) → Cyber (R)	4.01	0.05
Kinetic (R) → Cyber (R)	0.00	1.00
Cyber (U) → Cyber (R)	3.81	0.05



Table 12: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 2.** ‘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)	8.61	0.00
Cyber (U) → Kinetic (U)	0.97	0.33
Cyber (R) → Kinetic (U)	0.01	0.92
Kinetic (U) → Kinetic (R)	1.49	0.23
Cyber (U) → Kinetic (R)	0.75	0.39
Cyber (R) → Kinetic (R)	1.17	0.28
Kinetic (U) → Cyber (U)	0.61	0.44
Kinetic (R) → Cyber (U)	0.82	0.37
Cyber (R) → Cyber (U)	1.45	0.23
Kinetic (U) → Cyber (R)	6.79	0.01
Kinetic (R) → Cyber (R)	3.98	0.05
Cyber (U) → Cyber (R)	1.53	0.22

Table 13: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 2.** ‘U’ indicates reported 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	0.982	0.018	0.000	0.000
7 days	0.974	0.026	0.000	0.000
30 days	0.974	0.026	0.000	0.000
Kinetic (R)				
1 day	0.121	0.879	0.000	0.000
2 days	0.162	0.833	0.005	0.001
7 days	0.175	0.819	0.005	0.001
30 days	0.175	0.819	0.005	0.001
Cyber (U)				
1 day	0.002	0.000	0.998	0.000
2 days	0.003	0.001	0.996	0.000
7 days	0.004	0.001	0.995	0.000
30 days	0.004	0.001	0.995	0.000
Cyber (R)				
1 day	0.000	0.000	0.001	0.998
2 days	0.000	0.000	0.002	0.997
7 days	0.000	0.000	0.003	0.997
30 days	0.000	0.000	0.003	0.997

Table 14: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 2.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.936	0.053	0.011	0.001
6 weeks	0.896	0.086	0.017	0.001
12 weeks	0.894	0.088	0.017	0.001
Kinetic (R)				
1 week	0.263	0.737	0.000	0.000
2 weeks	0.386	0.611	0.002	0.001
6 weeks	0.461	0.535	0.002	0.002
12 weeks	0.464	0.532	0.002	0.002
Cyber (U)				
1 week	0.000	0.006	0.993	0.000
2 weeks	0.019	0.006	0.974	0.002
6 weeks	0.044	0.006	0.947	0.003
12 weeks	0.046	0.007	0.945	0.003
Cyber (R)				
1 week	0.015	0.000	0.017	0.968
2 weeks	0.015	0.023	0.018	0.944
6 weeks	0.021	0.028	0.018	0.933
12 weeks	0.021	0.028	0.018	0.933

### 10.3 Test 3: ‘Disruption’ cyber operations and physical violence in Ukraine from August 17, 2013 to February 29, 2016

Figure 12: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 3**. 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.

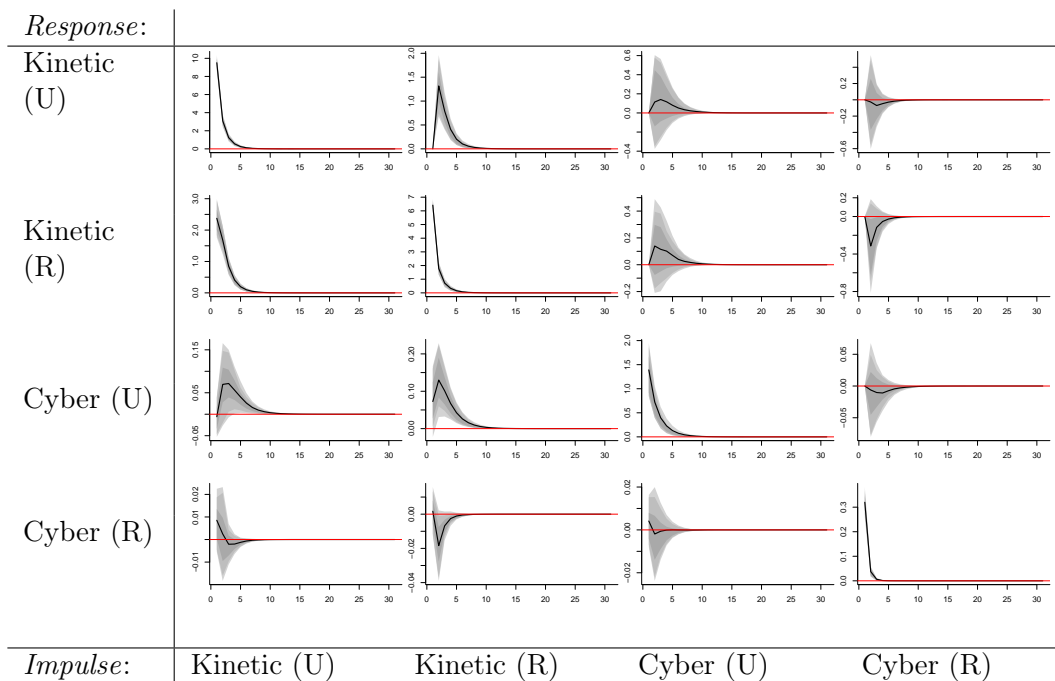


Figure 13: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 3**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

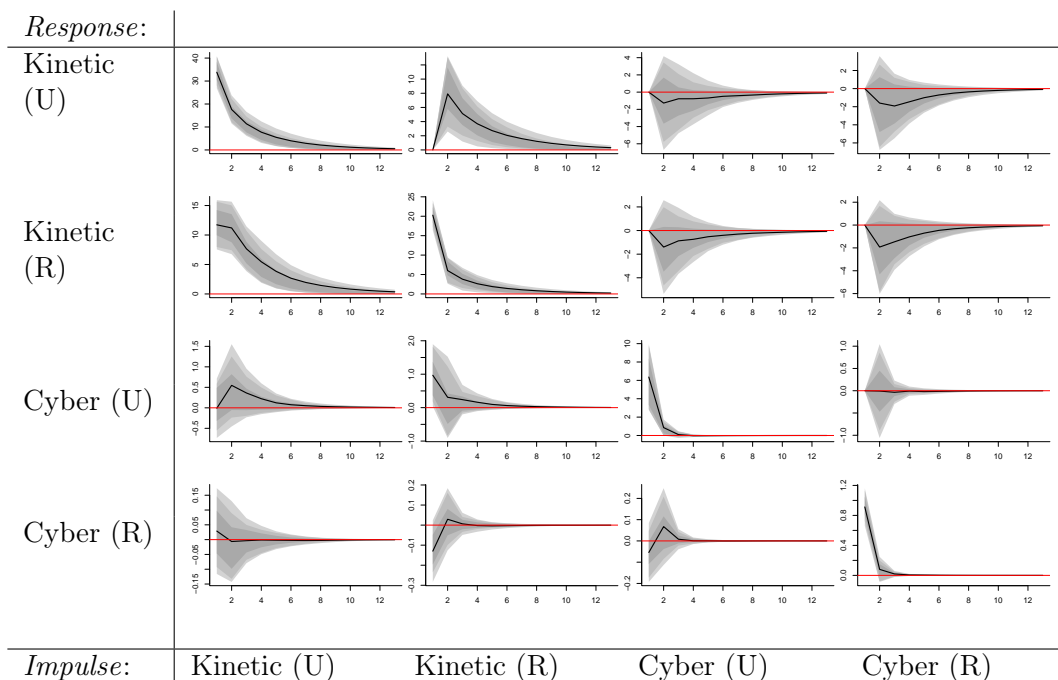


Table 15: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 3**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	20.85	0.00
Cyber (U) → Kinetic (U)	3.70	0.05
Cyber (R) → Kinetic (U)	2.06	0.15
Kinetic (U) → Kinetic (R)	15.99	0.00
Cyber (U) → Kinetic (R)	6.21	0.01
Cyber (R) → Kinetic (R)	1.79	0.18
Kinetic (U) → Cyber (U)	5.29	0.02
Kinetic (R) → Cyber (U)	14.45	0.00
Cyber (R) → Cyber (U)	0.15	0.70
Kinetic (U) → Cyber (R)	2.59	0.11
Kinetic (R) → Cyber (R)	3.10	0.08
Cyber (U) → Cyber (R)	1.46	0.23

Table 16: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 3.** ‘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)	8.61	0.00
Cyber (U) → Kinetic (U)	0.78	0.38
Cyber (R) → Kinetic (U)	0.97	0.33
Kinetic (U) → Kinetic (R)	1.49	0.23
Cyber (U) → Kinetic (R)	0.40	0.53
Cyber (R) → Kinetic (R)	0.00	0.99
Kinetic (U) → Cyber (U)	1.66	0.20
Kinetic (R) → Cyber (U)	4.80	0.03
Cyber (R) → Cyber (U)	0.01	0.93
Kinetic (U) → Cyber (R)	3.42	0.07
Kinetic (R) → Cyber (R)	0.04	0.85
Cyber (U) → Cyber (R)	0.00	0.99

Table 17: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 3.** ‘U’ indicates reported 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	0.982	0.018	0.000	0.000
7 days	0.973	0.026	0.001	0.000
30 days	0.973	0.026	0.001	0.000
Kinetic (R)				
1 day	0.119	0.881	0.000	0.000
2 days	0.161	0.837	0.000	0.002
7 days	0.173	0.823	0.001	0.003
30 days	0.173	0.823	0.001	0.003
Cyber (U)				
1 day	0.000	0.003	0.997	0.000
2 days	0.002	0.010	0.989	0.000
7 days	0.005	0.015	0.979	0.000
30 days	0.005	0.015	0.979	0.000
Cyber (R)				
1 day	0.001	0.000	0.000	0.999
2 days	0.001	0.004	0.000	0.996
7 days	0.001	0.004	0.000	0.995
30 days	0.001	0.004	0.000	0.995

Table 18: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 3.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.950	0.047	0.001	0.002
6 weeks	0.912	0.079	0.003	0.005
12 weeks	0.910	0.081	0.003	0.006
Kinetic (R)				
1 week	0.248	0.752	0.000	0.000
2 weeks	0.372	0.620	0.003	0.006
6 weeks	0.445	0.541	0.005	0.009
12 weeks	0.448	0.538	0.005	0.009
Cyber (U)				
1 week	0.001	0.018	0.982	0.000
2 weeks	0.004	0.017	0.979	0.000
6 weeks	0.006	0.017	0.977	0.000
12 weeks	0.006	0.017	0.977	0.000
Cyber (R)				
1 week	0.000	0.014	0.004	0.981
2 weeks	0.001	0.014	0.005	0.980
6 weeks	0.001	0.014	0.005	0.980
12 weeks	0.001	0.014	0.005	0.980

## 10.4 Test 4: ‘Disruption’ & ‘both’ cyber operations and physical violence in Ukraine from August 17, 2013 to February 29, 2016

Figure 14: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 4**. 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.

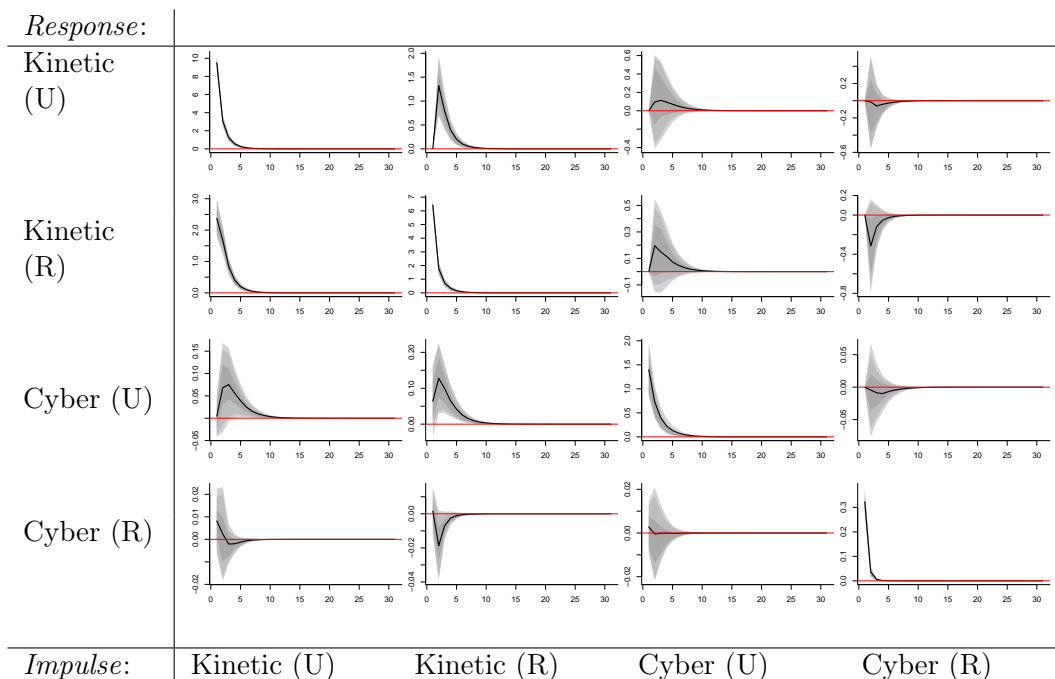


Figure 15: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 4**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

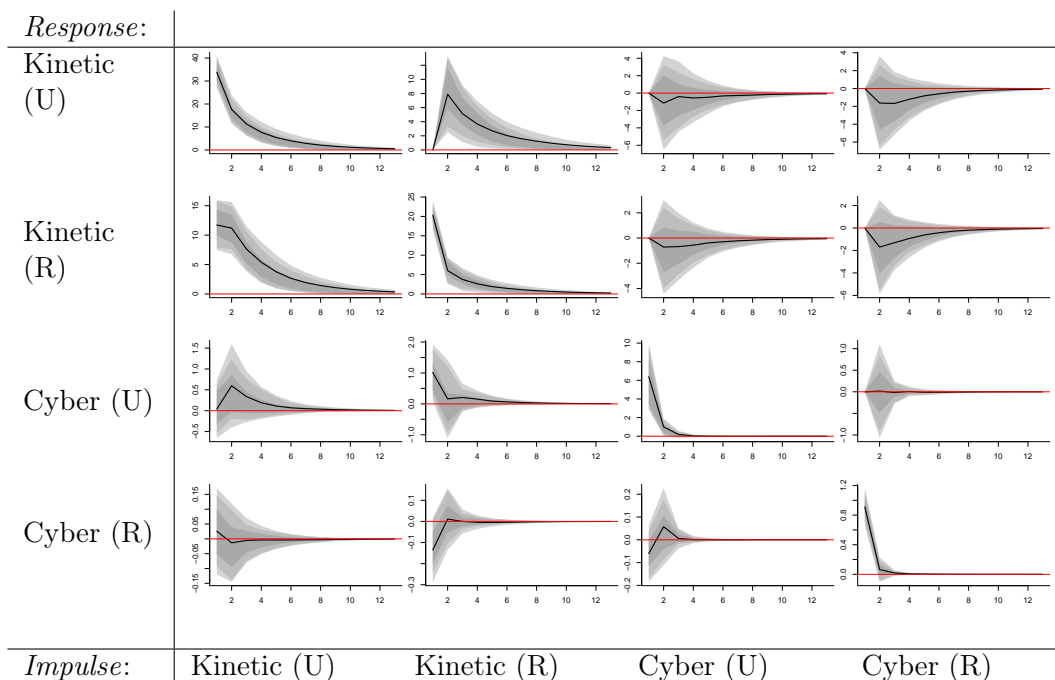


Table 19: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 4**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	20.85	0.00
Cyber (U) → Kinetic (U)	3.57	0.06
Cyber (R) → Kinetic (U)	2.25	0.13
Kinetic (U) → Kinetic (R)	15.99	0.00
Cyber (U) → Kinetic (R)	7.34	0.01
Cyber (R) → Kinetic (R)	1.99	0.16
Kinetic (U) → Cyber (U)	5.14	0.02
Kinetic (R) → Cyber (U)	14.17	0.00
Cyber (R) → Cyber (U)	0.10	0.75
Kinetic (U) → Cyber (R)	2.86	0.09
Kinetic (R) → Cyber (R)	3.39	0.07
Cyber (U) → Cyber (R)	1.38	0.24



Table 20: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 4.** ‘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)	8.61	0.00
Cyber (U) → Kinetic (U)	0.90	0.35
Cyber (R) → Kinetic (U)	0.99	0.32
Kinetic (U) → Kinetic (R)	1.49	0.23
Cyber (U) → Kinetic (R)	0.76	0.39
Cyber (R) → Kinetic (R)	0.00	0.95
Kinetic (U) → Cyber (U)	1.56	0.21
Kinetic (R) → Cyber (U)	4.06	0.05
Cyber (R) → Cyber (U)	0.01	0.92
Kinetic (U) → Cyber (R)	3.84	0.05
Kinetic (R) → Cyber (R)	0.09	0.76
Cyber (U) → Cyber (R)	0.01	0.93

Table 21: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 4.** ‘U’ indicates reported 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	0.982	0.018	0.000	0.000
7 days	0.973	0.026	0.001	0.000
30 days	0.973	0.026	0.001	0.000
Kinetic (R)				
1 day	0.119	0.881	0.000	0.000
2 days	0.160	0.837	0.000	0.002
7 days	0.173	0.823	0.001	0.003
30 days	0.173	0.823	0.001	0.003
Cyber (U)				
1 day	0.000	0.002	0.998	0.000
2 days	0.002	0.009	0.989	0.000
7 days	0.006	0.014	0.980	0.000
30 days	0.006	0.014	0.980	0.000
Cyber (R)				
1 day	0.000	0.000	0.000	0.999
2 days	0.000	0.004	0.000	0.996
7 days	0.001	0.004	0.000	0.995
30 days	0.001	0.004	0.000	0.995

Table 22: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 4.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.950	0.048	0.001	0.002
6 weeks	0.913	0.080	0.002	0.005
12 weeks	0.912	0.082	0.002	0.005
Kinetic (R)				
1 week	0.248	0.752	0.000	0.000
2 weeks	0.372	0.622	0.001	0.004
6 weeks	0.446	0.545	0.002	0.007
12 weeks	0.449	0.542	0.002	0.007
Cyber (U)				
1 week	0.001	0.018	0.981	0.000
2 weeks	0.005	0.018	0.977	0.000
6 weeks	0.006	0.018	0.976	0.000
12 weeks	0.006	0.018	0.976	0.000
Cyber (R)				
1 week	0.000	0.016	0.005	0.979
2 weeks	0.001	0.016	0.006	0.978
6 weeks	0.001	0.016	0.006	0.978
12 weeks	0.001	0.016	0.006	0.978

## 10.5 Test 5: Cyber and kinetic operations during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015)

Figure 16: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 5**. 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.

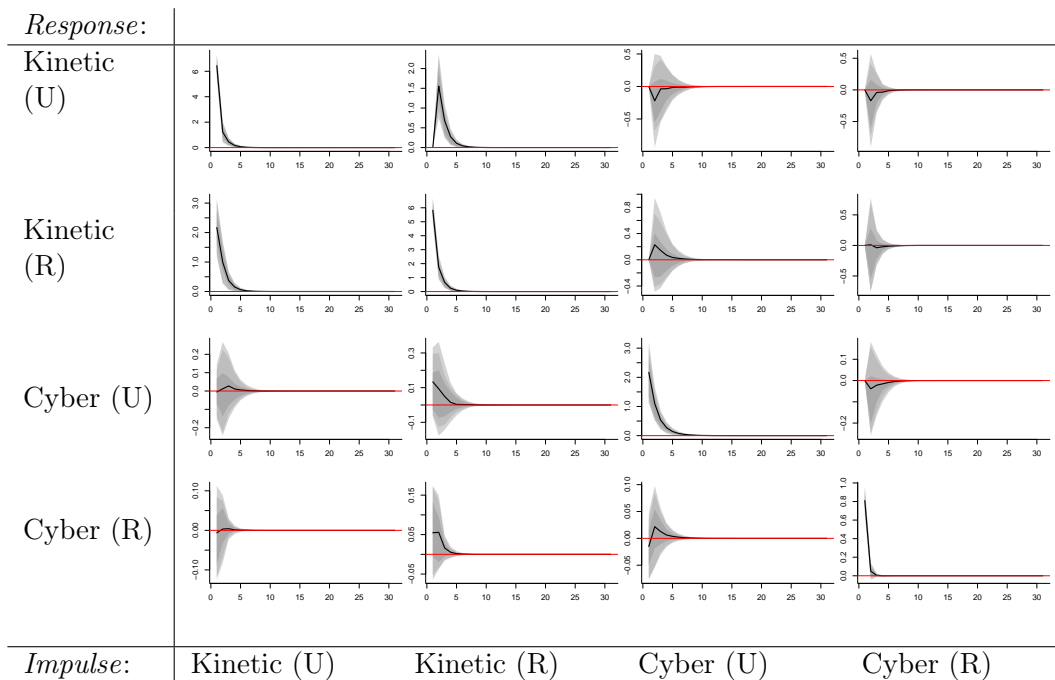


Figure 17: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 5**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

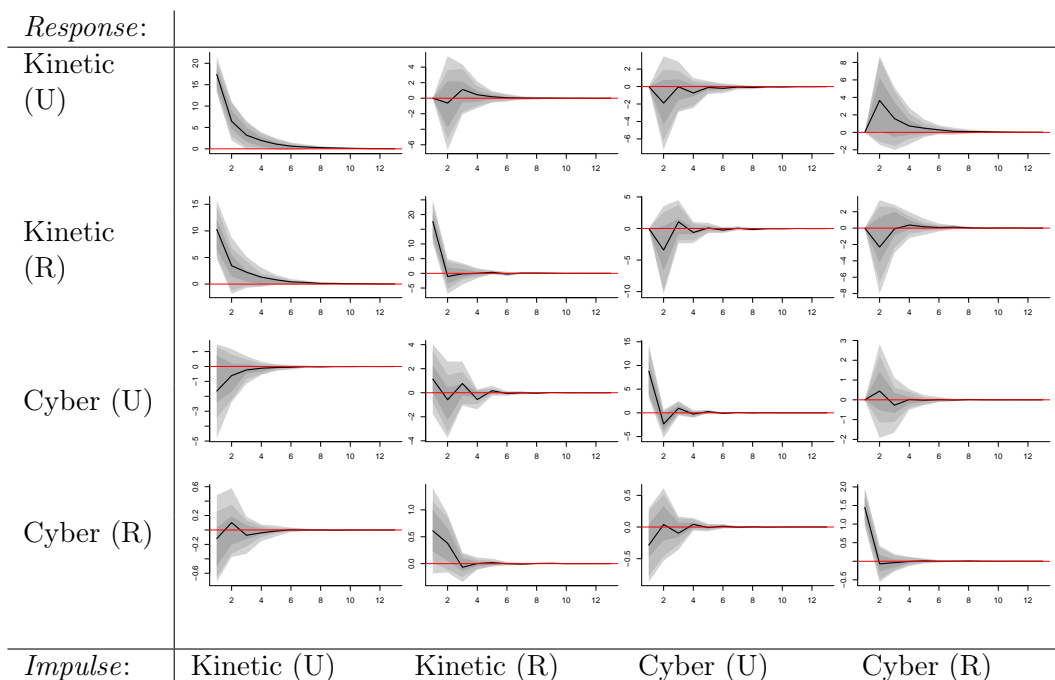


Table 23: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 5**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	40.26	0.00
Cyber (U) → Kinetic (U)	0.60	0.44
Cyber (R) → Kinetic (U)	0.10	0.75
Kinetic (U) → Kinetic (R)	12.29	0.00
Cyber (U) → Kinetic (R)	1.74	0.19
Cyber (R) → Kinetic (R)	1.49	0.22
Kinetic (U) → Cyber (U)	1.30	0.26
Kinetic (R) → Cyber (U)	1.61	0.21
Cyber (R) → Cyber (U)	0.84	0.36
Kinetic (U) → Cyber (R)	0.27	0.60
Kinetic (R) → Cyber (R)	0.23	0.63
Cyber (U) → Cyber (R)	0.39	0.53

Table 24: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 5.** ‘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)	0.23	0.63
Cyber (U) → Kinetic (U)	0.04	0.85
Cyber (R) → Kinetic (U)	1.15	0.29
Kinetic (U) → Kinetic (R)	3.89	0.06
Cyber (U) → Kinetic (R)	0.00	0.97
Cyber (R) → Kinetic (R)	1.42	0.24
Kinetic (U) → Cyber (U)	1.43	0.24
Kinetic (R) → Cyber (U)	1.66	0.21
Cyber (R) → Cyber (U)	0.59	0.45
Kinetic (U) → Cyber (R)	0.75	0.39
Kinetic (R) → Cyber (R)	1.35	0.25
Cyber (U) → Cyber (R)	0.59	0.45

Table 25: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 5.** ‘U’ indicates reported 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	0.937	0.060	0.002	0.002
7 days	0.925	0.071	0.002	0.002
30 days	0.925	0.071	0.002	0.002
Kinetic (R)				
1 day	0.113	0.887	0.000	0.000
2 days	0.126	0.873	0.000	0.001
7 days	0.128	0.871	0.000	0.001
30 days	0.128	0.871	0.000	0.001
Cyber (U)				
1 day	0.000	0.002	0.998	0.000
2 days	0.000	0.002	0.998	0.000
7 days	0.000	0.002	0.998	0.001
30 days	0.000	0.002	0.998	0.001
Cyber (R)				
1 day	0.001	0.005	0.000	0.994
2 days	0.001	0.008	0.001	0.991
7 days	0.001	0.008	0.001	0.990
30 days	0.001	0.008	0.001	0.990

Table 26: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 5.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.966	0.001	0.015	0.018
6 weeks	0.958	0.002	0.015	0.026
12 weeks	0.958	0.002	0.015	0.026
Kinetic (R)				
1 week	0.265	0.735	0.000	0.000
2 weeks	0.283	0.667	0.039	0.011
6 weeks	0.291	0.658	0.039	0.012
12 weeks	0.291	0.658	0.039	0.012
Cyber (U)				
1 week	0.008	0.009	0.983	0.000
2 weeks	0.016	0.014	0.965	0.004
6 weeks	0.017	0.015	0.964	0.004
12 weeks	0.017	0.015	0.964	0.004
Cyber (R)				
1 week	0.024	0.141	0.012	0.824
2 weeks	0.023	0.178	0.012	0.787
6 weeks	0.024	0.178	0.012	0.786
12 weeks	0.024	0.178	0.012	0.786

## 10.6 Test 6: ‘Propaganda’ cyber operations and physical violence during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015)

Figure 18: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 6**. 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.

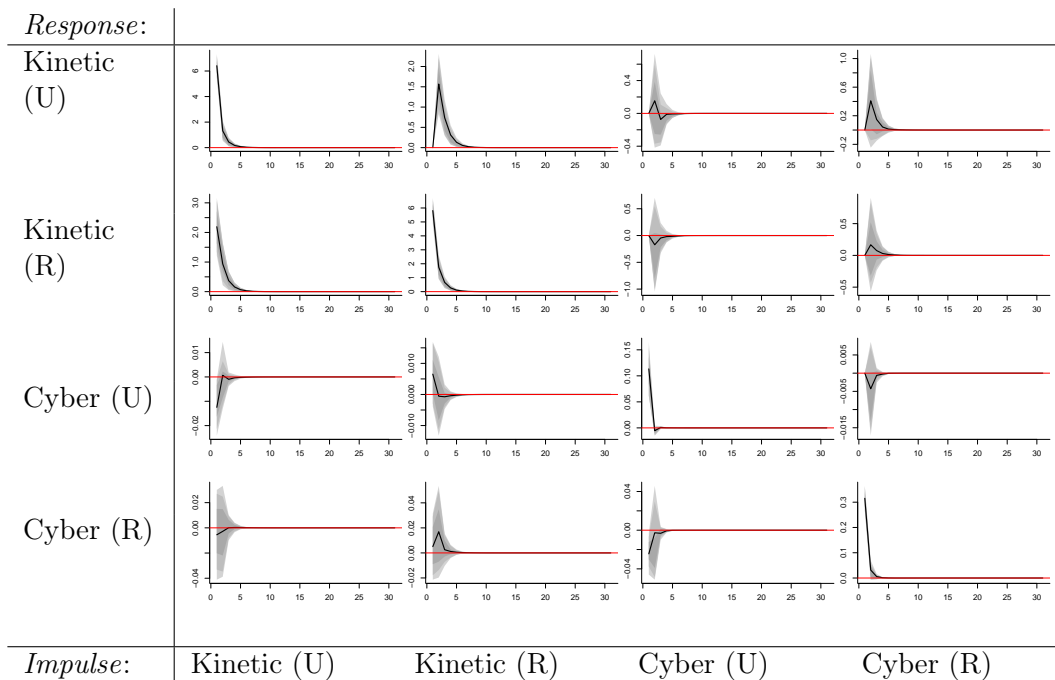


Figure 19: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 6**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

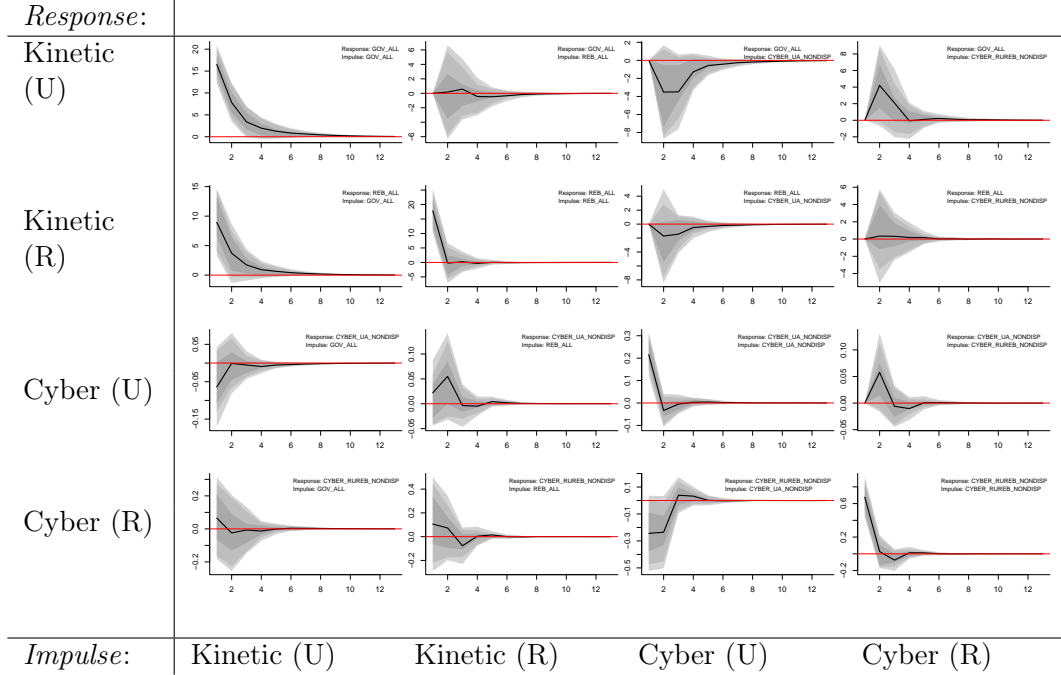


Table 27: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 6**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	40.26	0.00
Cyber (U) → Kinetic (U)	0.40	0.53
Cyber (R) → Kinetic (U)	0.11	0.74
Kinetic (U) → Kinetic (R)	12.29	0.00
Cyber (U) → Kinetic (R)	1.97	0.16
Cyber (R) → Kinetic (R)	0.61	0.44
Kinetic (U) → Cyber (U)	0.71	0.40
Kinetic (R) → Cyber (U)	1.00	0.32
Cyber (R) → Cyber (U)	0.51	0.48
Kinetic (U) → Cyber (R)	3.51	0.06
Kinetic (R) → Cyber (R)	2.06	0.15
Cyber (U) → Cyber (R)	0.37	0.54



Table 28: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 6.** ‘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)	0.23	0.63
Cyber (U) → Kinetic (U)	0.26	0.61
Cyber (R) → Kinetic (U)	0.26	0.61
Kinetic (U) → Kinetic (R)	3.89	0.06
Cyber (U) → Kinetic (R)	0.27	0.60
Cyber (R) → Kinetic (R)	0.86	0.36
Kinetic (U) → Cyber (U)	0.87	0.36
Kinetic (R) → Cyber (U)	0.32	0.58
Cyber (R) → Cyber (U)	2.20	0.15
Kinetic (U) → Cyber (R)	3.04	0.09
Kinetic (R) → Cyber (R)	3.96	0.05
Cyber (U) → Cyber (R)	0.11	0.74

Table 29: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 6.** ‘U’ indicates reported 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	0.936	0.059	0.000	0.004
7 days	0.923	0.072	0.001	0.005
30 days	0.923	0.072	0.001	0.005
Kinetic (R)				
1 day	0.113	0.887	0.000	0.000
2 days	0.126	0.870	0.004	0.000
7 days	0.128	0.867	0.004	0.000
30 days	0.128	0.867	0.004	0.000
Cyber (U)				
1 day	0.008	0.003	0.989	0.000
2 days	0.009	0.003	0.983	0.005
7 days	0.009	0.003	0.983	0.005
30 days	0.009	0.003	0.983	0.005
Cyber (R)				
1 day	0.000	0.000	0.005	0.995
2 days	0.000	0.003	0.001	0.987
7 days	0.000	0.003	0.001	0.987
30 days	0.000	0.003	0.001	0.987

Table 30: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 6.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.900	0.001	0.054	0.044
6 weeks	0.852	0.007	0.087	0.054
12 weeks	0.852	0.007	0.088	0.054
Kinetic (R)				
1 week	0.240	0.760	0.000	0.000
2 weeks	0.262	0.718	0.016	0.003
6 weeks	0.269	0.705	0.021	0.004
12 weeks	0.269	0.705	0.021	0.004
Cyber (U)				
1 week	0.034	0.000	0.965	0.000
2 weeks	0.036	0.047	0.895	0.022
6 weeks	0.040	0.048	0.890	0.023
12 weeks	0.040	0.048	0.890	0.023
Cyber (R)				
1 week	0.005	0.034	0.118	0.843
2 weeks	0.004	0.031	0.201	0.763
6 weeks	0.005	0.034	0.200	0.761
12 weeks	0.004	0.034	0.200	0.761

## 10.7 Test 7: ‘Disruption’ cyber operations and physical violence during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015)

Figure 20: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 7**. 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.

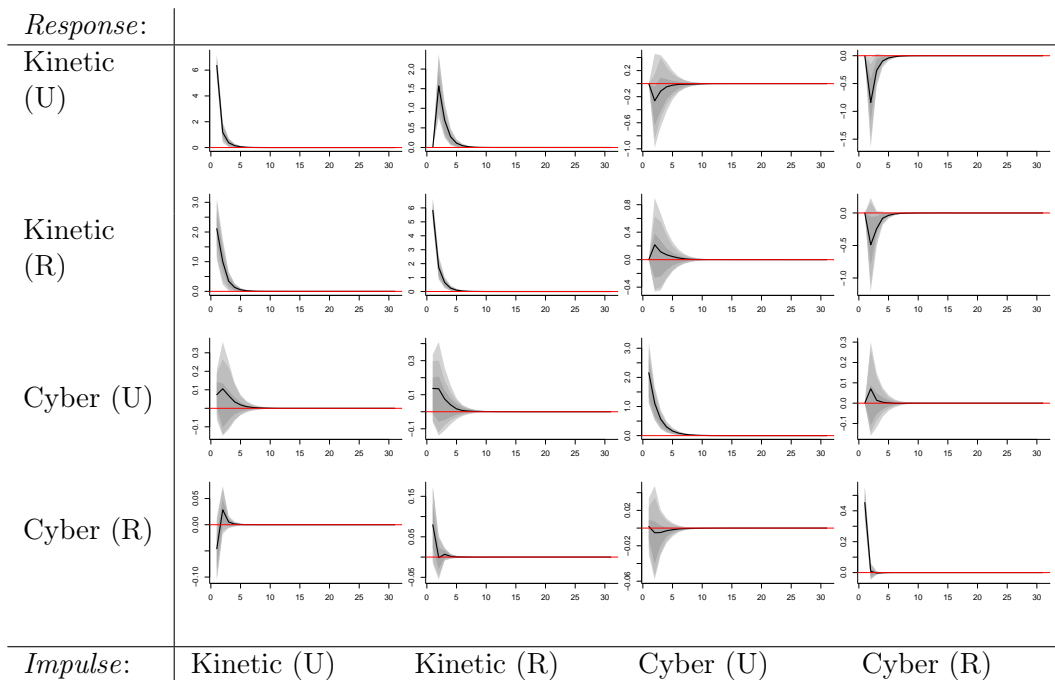


Figure 21: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 7**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

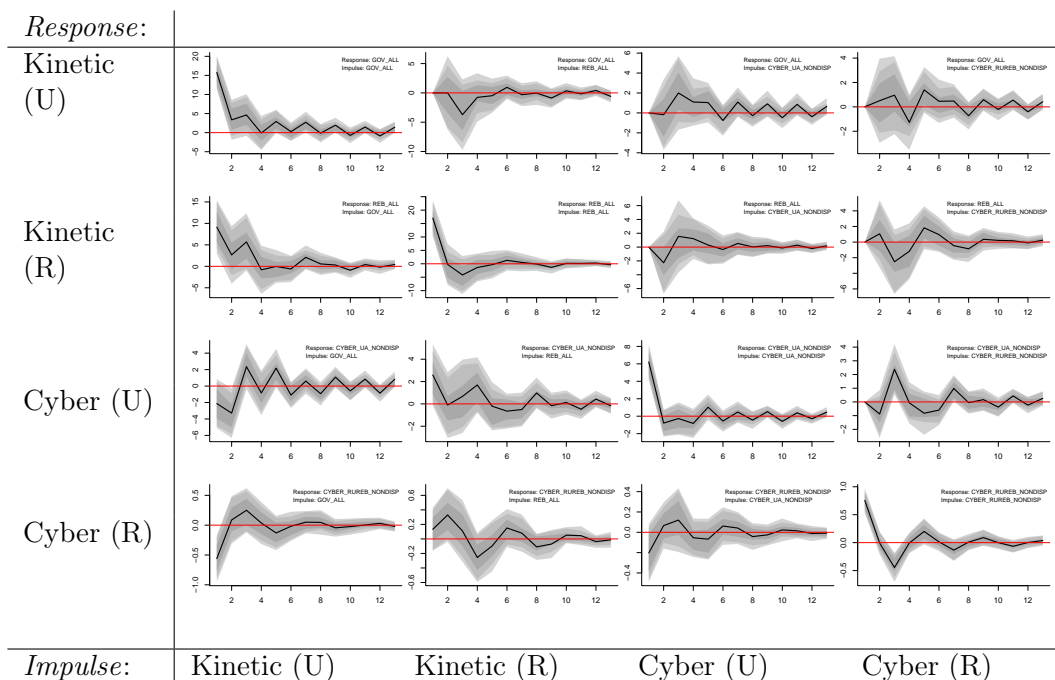


Table 31: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 7**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	F-statistic	p-value
Kinetic (R) → Kinetic (U)	40.26	0.00
Cyber (U) → Kinetic (U)	0.15	0.70
Cyber (R) → Kinetic (U)	0.09	0.76
Kinetic (U) → Kinetic (R)	12.29	0.00
Cyber (U) → Kinetic (R)	1.33	0.25
Cyber (R) → Kinetic (R)	2.70	0.10
Kinetic (U) → Cyber (U)	1.08	0.30
Kinetic (R) → Cyber (U)	1.34	0.25
Cyber (R) → Cyber (U)	0.03	0.86
Kinetic (U) → Cyber (R)	1.74	0.19
Kinetic (R) → Cyber (R)	0.14	0.71
Cyber (U) → Cyber (R)	0.83	0.36

Table 32: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 7.** ‘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)	0.12	0.89
Cyber (U) → Kinetic (U)	0.69	0.51
Cyber (R) → Kinetic (U)	1.30	0.28
Kinetic (U) → Kinetic (R)	1.07	0.35
Cyber (U) → Kinetic (R)	0.51	0.60
Cyber (R) → Kinetic (R)	0.19	0.83
Kinetic (U) → Cyber (U)	7.28	0.00
Kinetic (R) → Cyber (U)	3.14	0.06
Cyber (R) → Cyber (U)	0.46	0.63
Kinetic (U) → Cyber (R)	1.01	0.37
Kinetic (R) → Cyber (R)	0.24	0.79
Cyber (U) → Cyber (R)	0.06	0.94

Table 33: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 7.** ‘U’ indicates reported 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	0.919	0.060	0.003	0.018
7 days	0.904	0.072	0.004	0.020
30 days	0.904	0.072	0.004	0.020
Kinetic (R)				
1 day	0.109	0.891	0.000	0.000
2 days	0.121	0.872	0.000	0.006
7 days	0.123	0.869	0.000	0.008
30 days	0.123	0.869	0.000	0.008
Cyber (U)				
1 day	0.001	0.001	0.997	0.000
2 days	0.001	0.002	0.997	0.000
7 days	0.001	0.002	0.997	0.000
30 days	0.001	0.002	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 34: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 7.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.994	0.000	0.005	0.000
6 weeks	0.943	0.030	0.019	0.008
12 weeks	0.940	0.030	0.021	0.009
Kinetic (R)				
1 week	0.248	0.752	0.000	0.000
2 weeks	0.258	0.726	0.015	0.001
6 weeks	0.291	0.667	0.014	0.028
12 weeks	0.291	0.664	0.015	0.029
Cyber (U)				
1 week	0.109	0.110	0.781	0.000
2 weeks	0.311	0.084	0.597	0.009
6 weeks	0.340	0.095	0.499	0.066
12 weeks	0.343	0.097	0.489	0.071
Cyber (R)				
1 week	0.290	0.019	0.045	0.646
2 weeks	0.263	0.102	0.047	0.588
6 weeks	0.224	0.130	0.061	0.585
12 weeks	0.221	0.132	0.063	0.584

## 10.8 Test 8: ‘Disruption’ & ‘both’ cyber operations and physical violence during the ‘fighting’ period in Ukraine (5/11/2014-2/15/2015)

Figure 22: IMPULSE-RESPONSE MATRIX, DAILY TIME SERIES. **TEST 8**. 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.

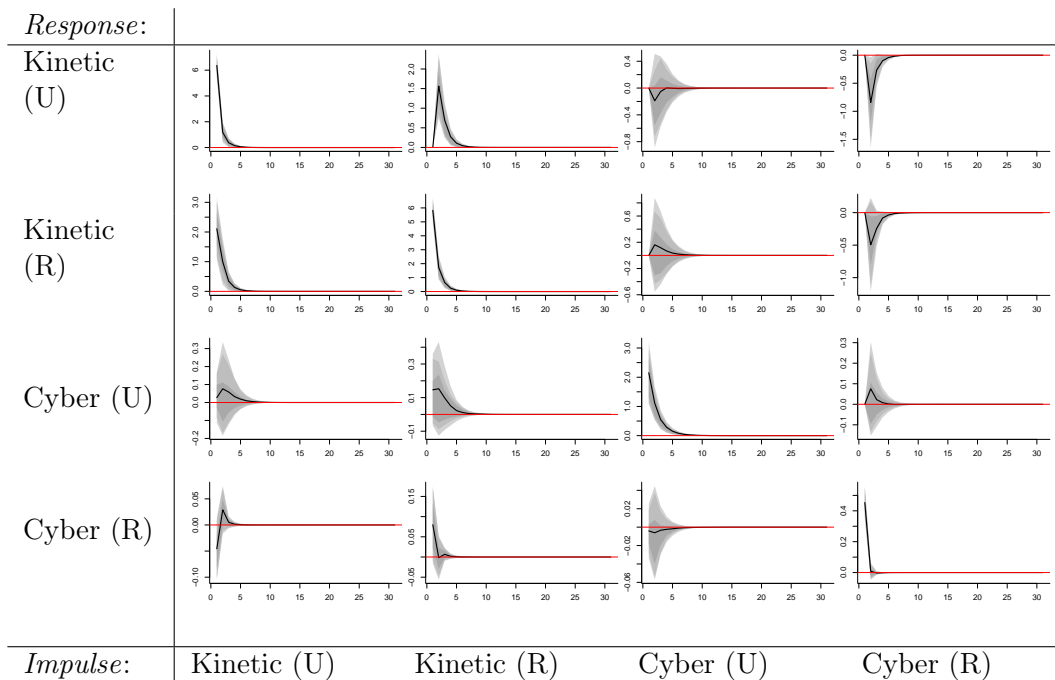


Figure 23: IMPULSE-RESPONSE MATRIX, WEEKLY TIME SERIES. **TEST 8**. Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

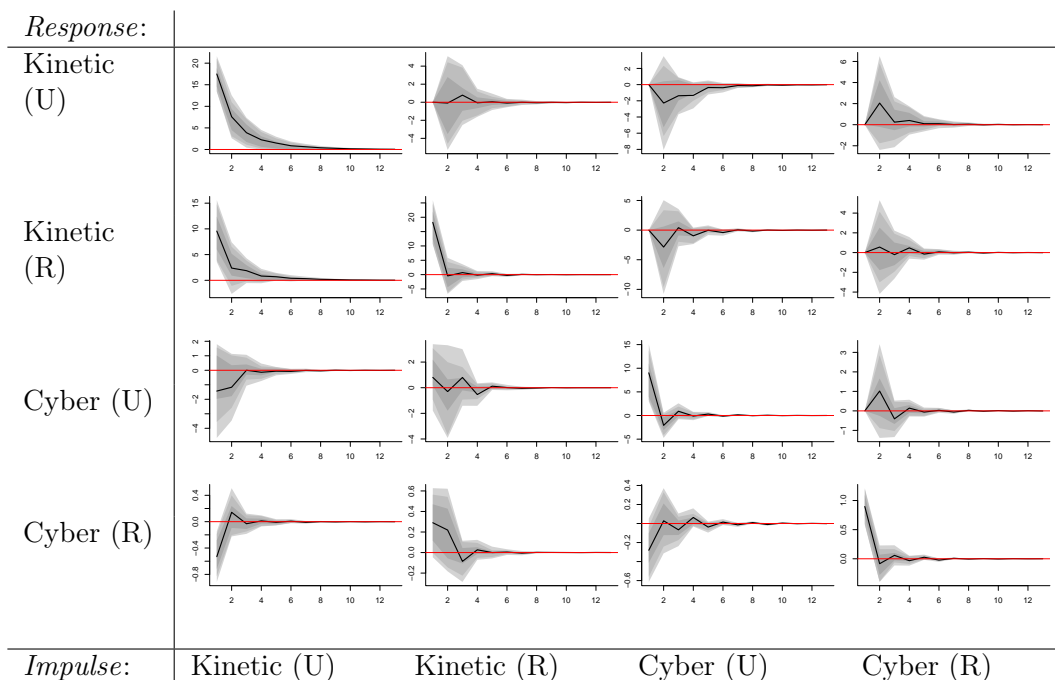


Table 35: GRANGER CAUSALITY TEST, DAILY TIME SERIES. **TEST 8**. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

	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 36: GRANGER CAUSALITY TEST, WEEKLY TIME SERIES. **TEST 8.** ‘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)	0.23	0.63
Cyber (U) → Kinetic (U)	0.03	0.87
Cyber (R) → Kinetic (U)	2.36	0.13
Kinetic (U) → Kinetic (R)	3.89	0.06
Cyber (U) → Kinetic (R)	0.00	0.97
Cyber (R) → Kinetic (R)	0.03	0.87
Kinetic (U) → Cyber (U)	1.50	0.23
Kinetic (R) → Cyber (U)	1.68	0.20
Cyber (R) → Cyber (U)	0.20	0.66
Kinetic (U) → Cyber (R)	0.12	0.73
Kinetic (R) → Cyber (R)	1.05	0.82
Cyber (U) → Cyber (R)	0.05	0.83

Table 37: VARIANCE DECOMPOSITION, DAILY TIME SERIES. **TEST 8.** ‘U’ indicates reported 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 38: VARIANCE DECOMPOSITION, WEEKLY TIME SERIES. **TEST 8.** ‘U’ indicates reported 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 week	1.000	0.000	0.000	0.000
2 weeks	0.982	0.002	0.014	0.003
6 weeks	0.980	0.001	0.016	0.003
12 weeks	0.980	0.001	0.016	0.003
Kinetic (R)				
1 week	0.238	0.762	0.000	0.000
2 weeks	0.289	0.719	0.028	0.001
6 weeks	0.126	0.711	0.029	0.001
12 weeks	0.214	0.711	0.029	0.001
Cyber (U)				
1 week	0.005	0.010	0.985	0.000
2 weeks	0.013	0.014	0.965	0.009
6 weeks	0.013	0.014	0.964	0.009
12 weeks	0.013	0.014	0.964	0.009
Cyber (R)				
1 week	0.181	0.055	0.041	0.723
2 weeks	0.171	0.106	0.039	0.684
6 weeks	0.171	0.106	0.040	0.683
12 weeks	0.171	0.106	0.040	0.683

Figure 24: IMPULSE-RESPONSE MATRIX WITH PERMUTED CAUSAL ORDERING, DAILY TIME SERIES. **TEST 8.** Black lines are point estimates and dotted lines are 95% confidence intervals, from 24 permutations of the ordering of the four endogenous variables. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

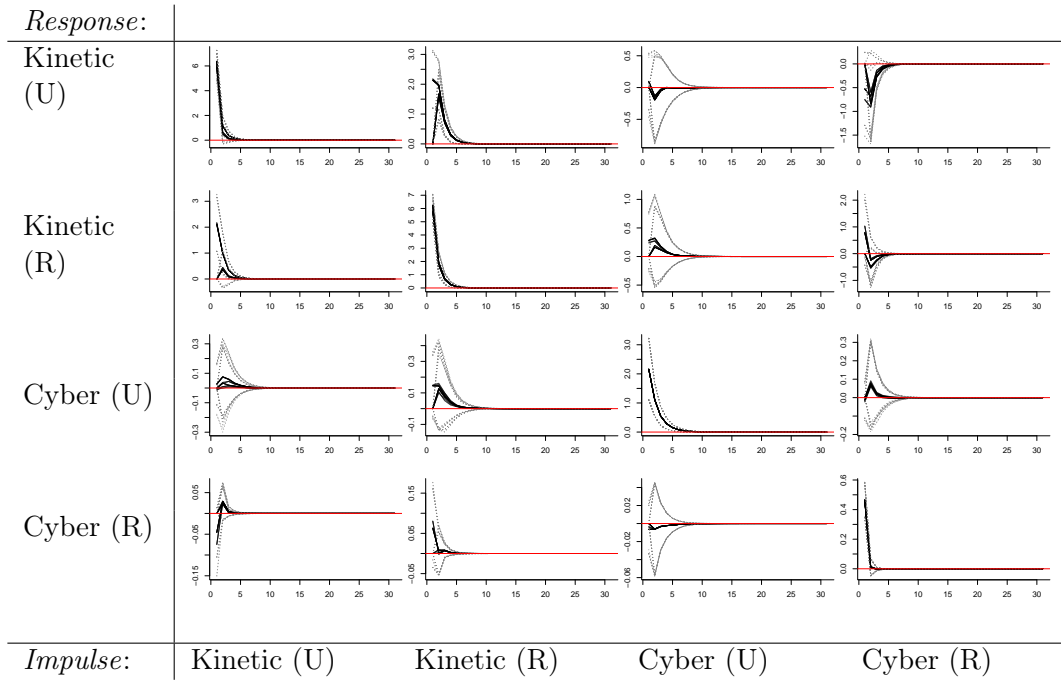


Figure 25: IMPULSE-RESPONSE MATRIX WITH PERMUTED CAUSAL ORDERING, WEEKLY TIME SERIES. **TEST 8**. Black lines are point estimates and dotted lines are 95% confidence intervals, from 24 permutations of the ordering of the four endogenous variables. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

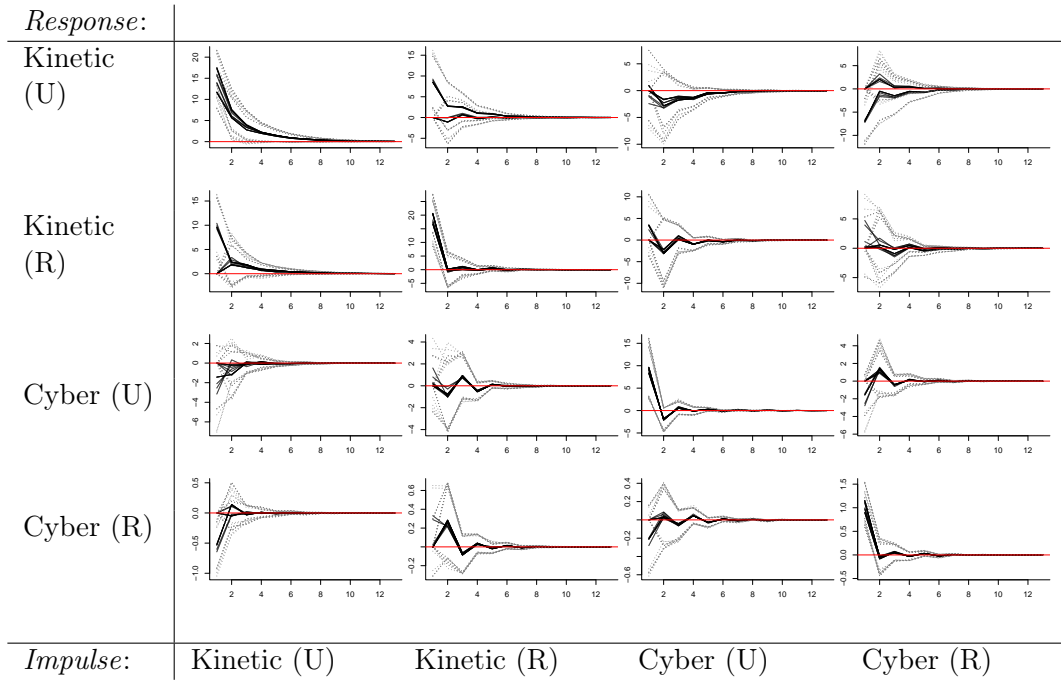


Figure 26: IMPULSE-RESPONSE MATRIX, RUSSIAN SOURCES, DAILY TIME SERIES. **TEST 8.** Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.

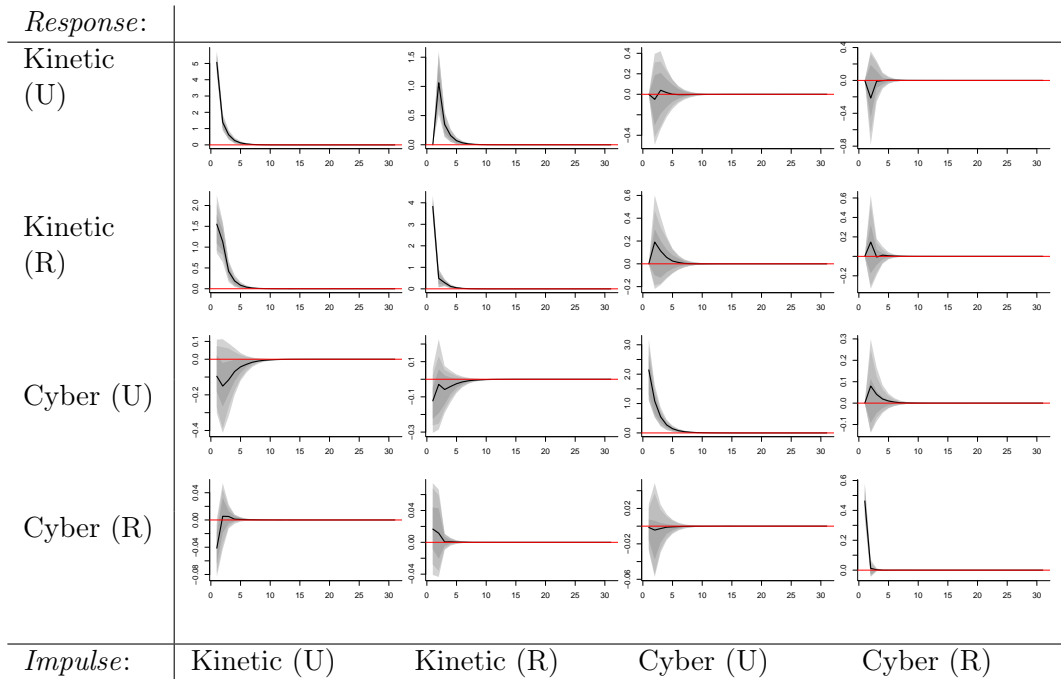
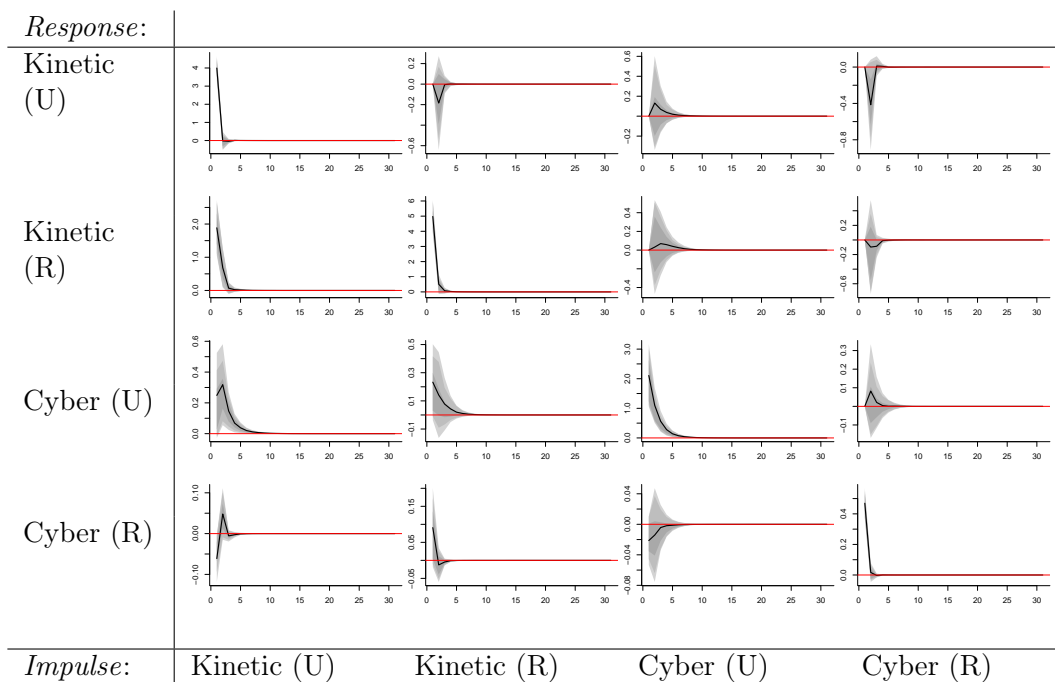


Figure 27: IMPULSE-RESPONSE MATRIX, UKRAINIAN SOURCES, DAILY TIME SERIES. **TEST 8.** Light grey area represents 95% confidence intervals, medium grey 90%, dark grey 68%. ‘U’ indicates reported kinetic and cyber operations by pro-Ukrainian government forces, and ‘R’ indicates operations by pro-Russian rebel forces.



## 11 Syria Results & Robustness Checks

In addition to the IRF curves in Figure 28, we run the variance decomposition results (Figure 39) and Granger tests (Figure 40). These results confirm our earlier findings – links between kinetic operations and their disconnect from cyber attacks.

Figure 28: 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.

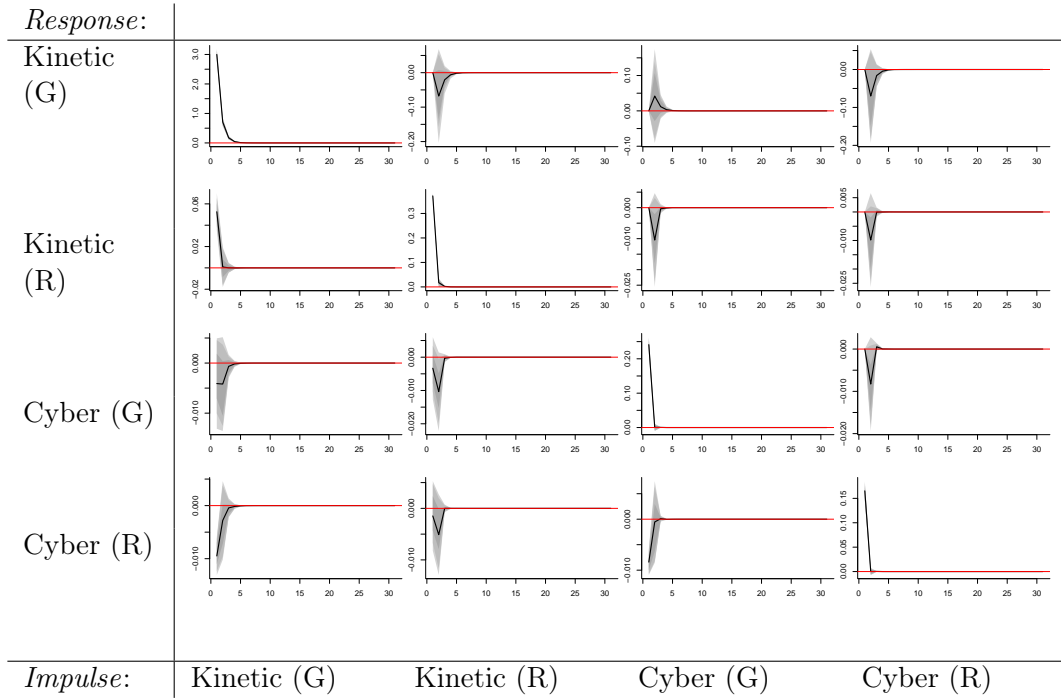


Table 39: VARIANCE DECOMPOSITION, DAILY TIME SERIES (SYRIA). ‘G’ indicates reported kinetic and cyber operations by pro-Assad government forces, and ‘R’ indicates operations by anti-Assad rebel forces.

	Kinetic (G)	Kinetic (R)	Cyber (R)	Cyber (G)
Kinetic (G)				
1 day	1.000	0.000	0.000	0.000
2 days	0.999	0.000	0.000	0.001
7 days	0.999	0.001	0.000	0.001
30 days	0.999	0.001	0.000	0.001
Kinetic (R)				
1 day	0.019	0.981	0.000	0.000
2 days	0.019	0.979	0.001	0.001
7 days	0.019	0.979	0.001	0.001
30 days	0.019	0.979	0.001	0.001
Cyber (R)				
1 day	0.000	0.000	1.000	0.000
2 days	0.000	0.002	0.996	0.001
7 days	0.000	0.002	0.996	0.001
30 days	0.000	0.002	0.996	0.001
Cyber (G)				
1 day	0.003	0.000	0.003	0.994
2 days	0.003	0.001	0.003	0.993
7 days	0.003	0.001	0.003	0.993
30 days	0.003	0.001	0.003	0.993

Table 40: GRANGER CAUSALITY TEST, DAILY TIME SERIES (SYRIA). ‘G’ indicates reported kinetic and cyber operations by pro-Assad government forces, and ‘R’ indicates operations by anti-Assad rebel forces.

	F-statistic	p-value
Kinetic (R) -> Kinetic (G)	9.11	0.00
Cyber (R) -> Kinetic (G)	0.12	0.73
Cyber (G) -> Kinetic (G)	2.24	0.13
Kinetic (G) -> Kinetic (R)	9.45	0.00
Cyber (R) -> Kinetic (R)	1.70	0.19
Cyber (G) -> Kinetic (R)	1.59	0.21
Kinetic (G) -> Cyber (R)	0.50	0.48
Kinetic (R) -> Cyber (R)	3.48	0.06
Cyber (G) -> Cyber (R)	1.74	0.19
Kinetic (G) -> Cyber (G)	2.46	0.12
Kinetic (R) -> Cyber (G)	2.04	0.15
Cyber (R) -> Cyber (G)	0.03	0.87