Trends in Online Foreign Influence Efforts

August 14, 2019

Meysam Alizadeh, Diego A. Martin, Jacob N. Shapiro

PRINCETON UNIVERSITY

ESOC
Empirical Studies of Conflict

What is a Foreign Influence Effort (FIE)?

Three criteria:

1. Foreign, i.e. attempt by country A to project content in country B
2. Deceptive, i.e. masquerading as organic to country B
3. Political, i.e. clearly identifiable objective

53 FIE against 24 different countries since 2014

- 72% by Russia, most others by Iran
- Russian efforts: 14 vs. US, 3 vs. UK, 2 each vs. Australia, Germany, Netherlands, and Ukraine, and 1 each in 14 other countries
- Mean duration 2.2 years
- Wide variety of political goals
- At least 41 other influence efforts that met only some criteria

PRINCETON UNIVERSITY

FIE Example

ESOC Empirical Studies of Conflict

Project Lakhta (2014-present by Russia)

- Campaign to exploit social media platforms to influence politics in US, EU, Ukraine, and Russia, among others
- Goals for US:
  - "spread distrust towards candidates for political office and political system in general"
  - "political intensity through supporting radical groups"
  - "effectively aggravate the conflict between minorities and the rest of the population"
- IRA + 11 other Russian agencies involved
- Create fictitious personae across range of platforms

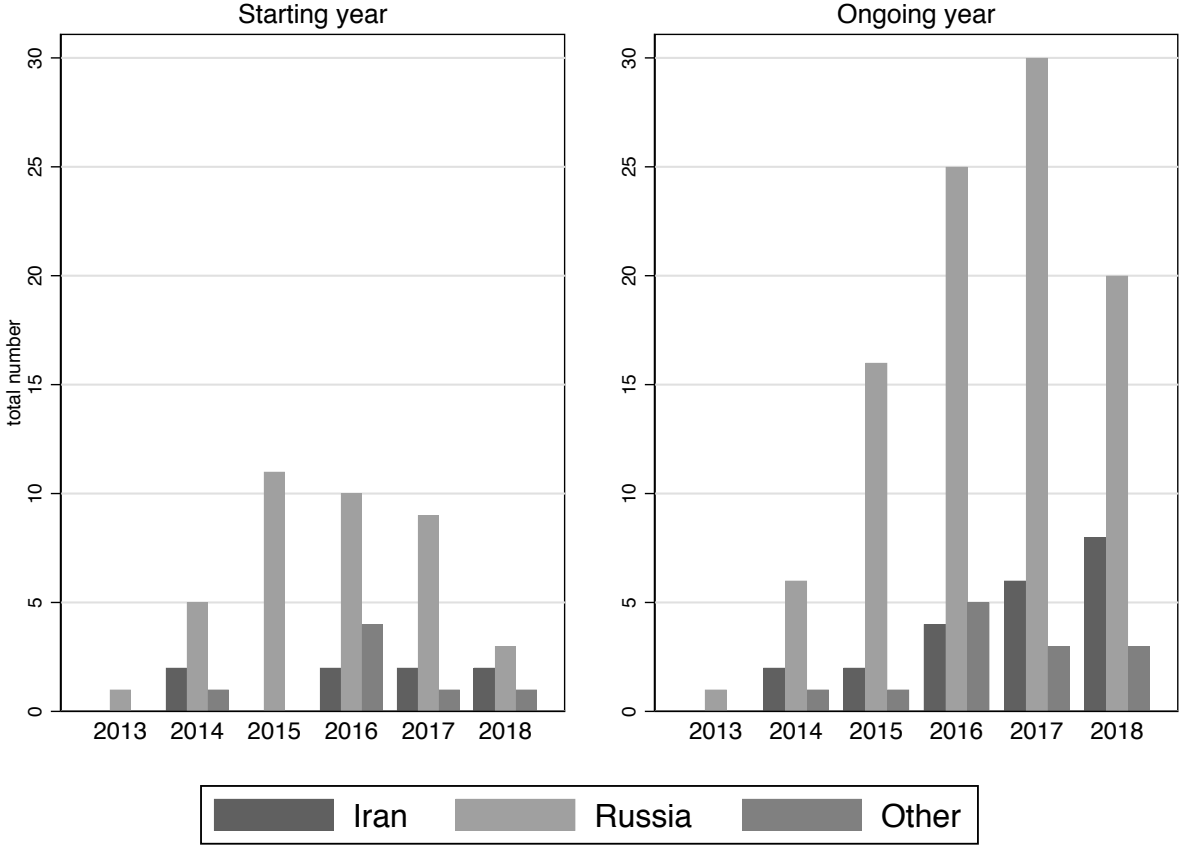
Source: Indictment of ELENA ALEKSEEVNA KHUSYAYNOVA, Sep. 28, 2018

Influence Effort Example

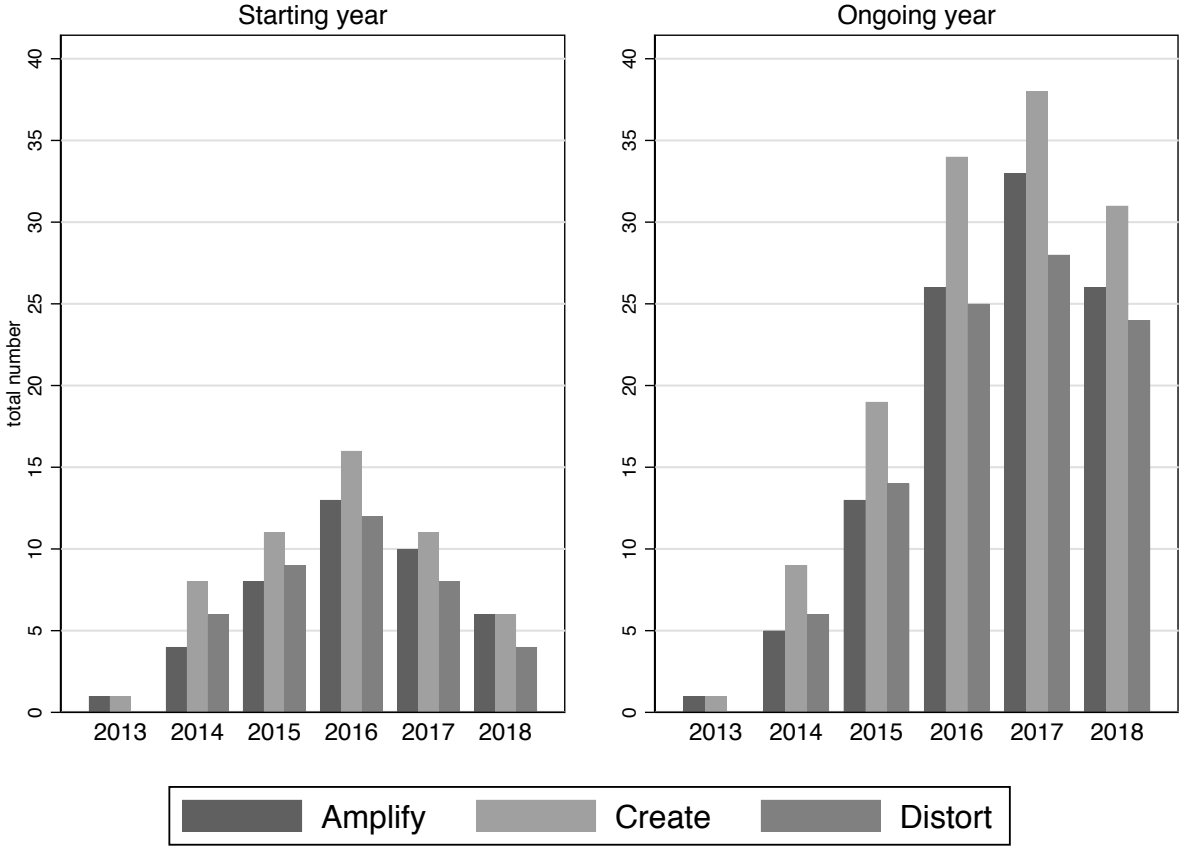
- In 2016, the Russian Federation operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (“GRU”). The GRU had multiple units, engaged in cyber operations.
- Antonov and others were GRU officers conspired to gain unauthorized access (to “hack”) into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election.
- Beginning in or around June 2016, the Conspirators staged and released tens of thousands of the stolen emails and documents. They did so using fictitious online personas, including “DCLeaks” and “Guccifer 2.0.

Source: Indictment of BORIS ALEKSEYEVICH ANTONOV and others, Jul. 13, 2018

Trends Over Time by Country



Trends Over Time by Approach

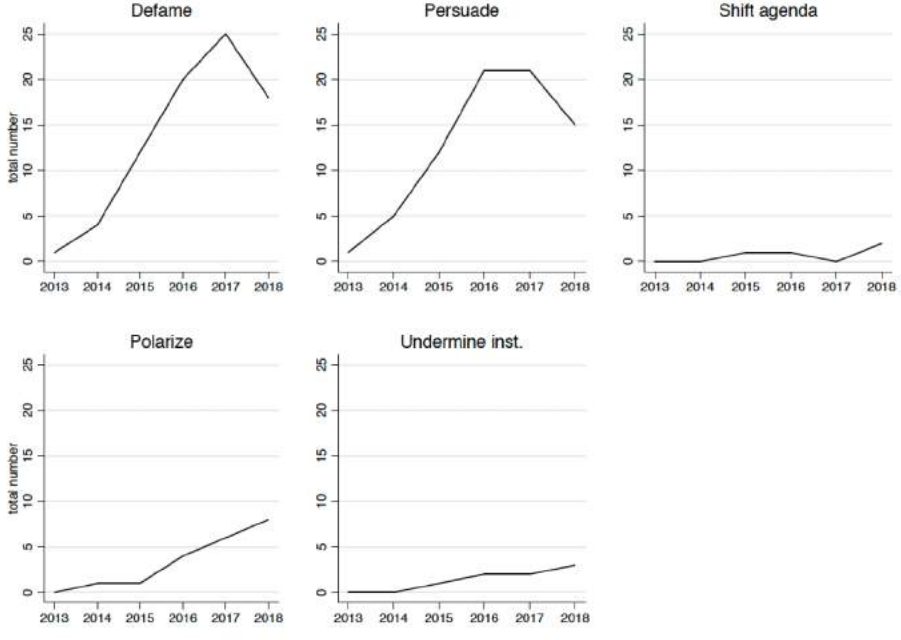


PRINCETON UNIVERSITY

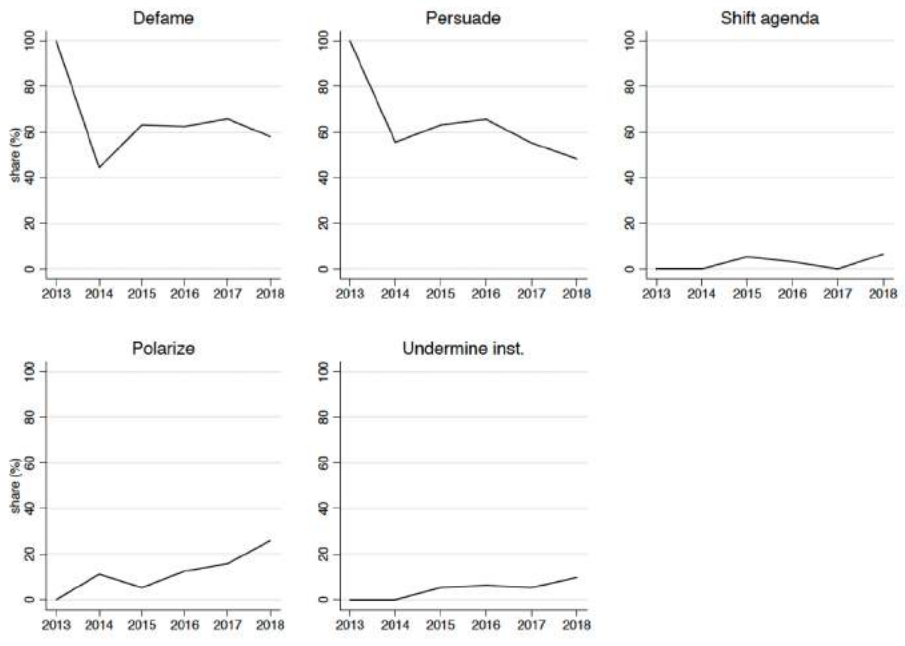
Trends in Strategy

ESOC
Empirical Studies of Conflict

Panel A: Total number of attacks per strategy



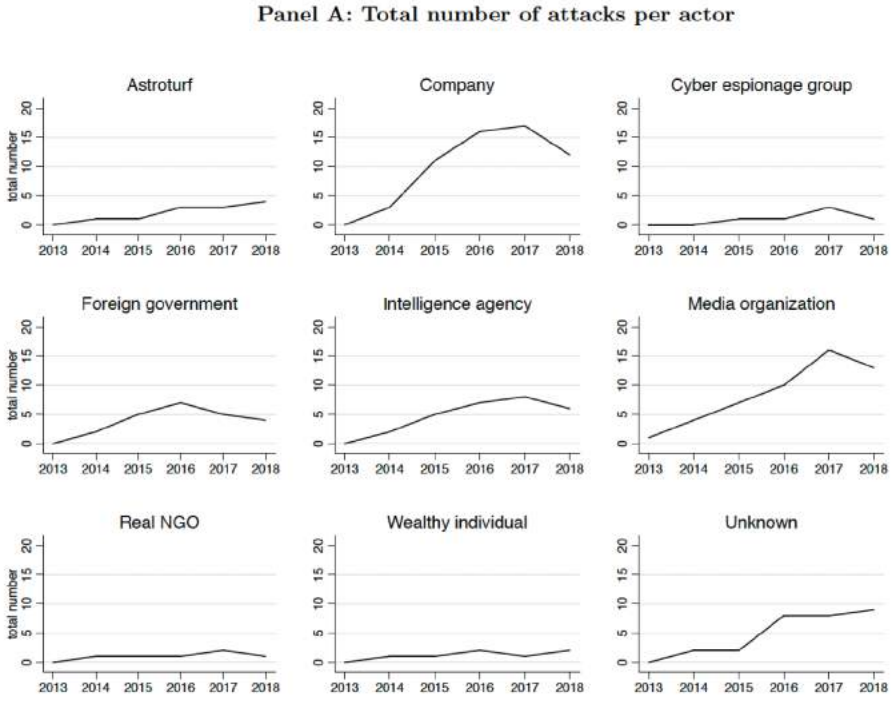
Panel B: Share of attacks involving strategies

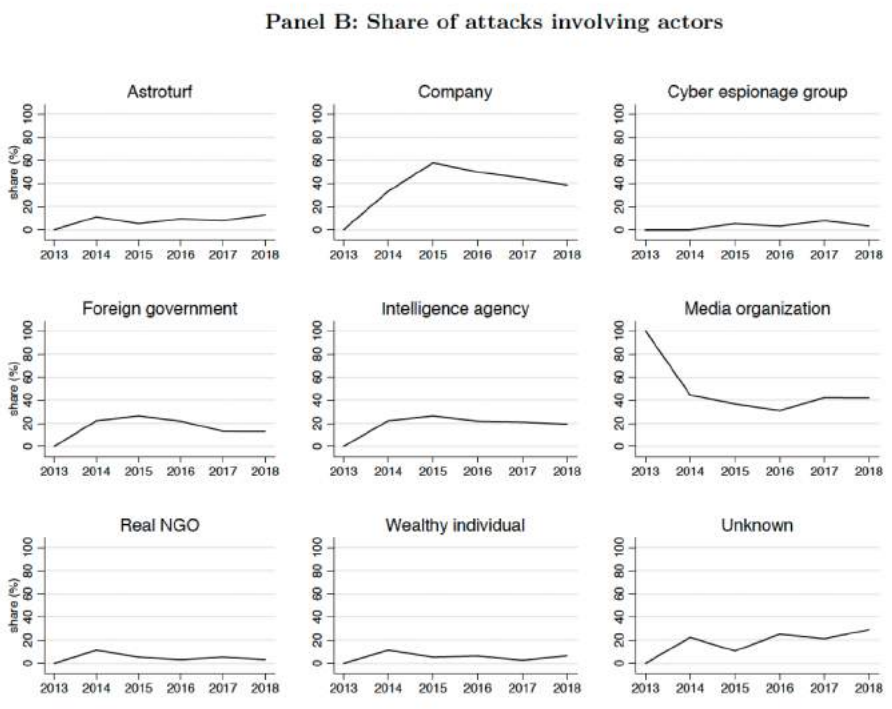


PRINCETON UNIVERSITY

Trends in Actors

ESOC Empirical Studies of Conflict

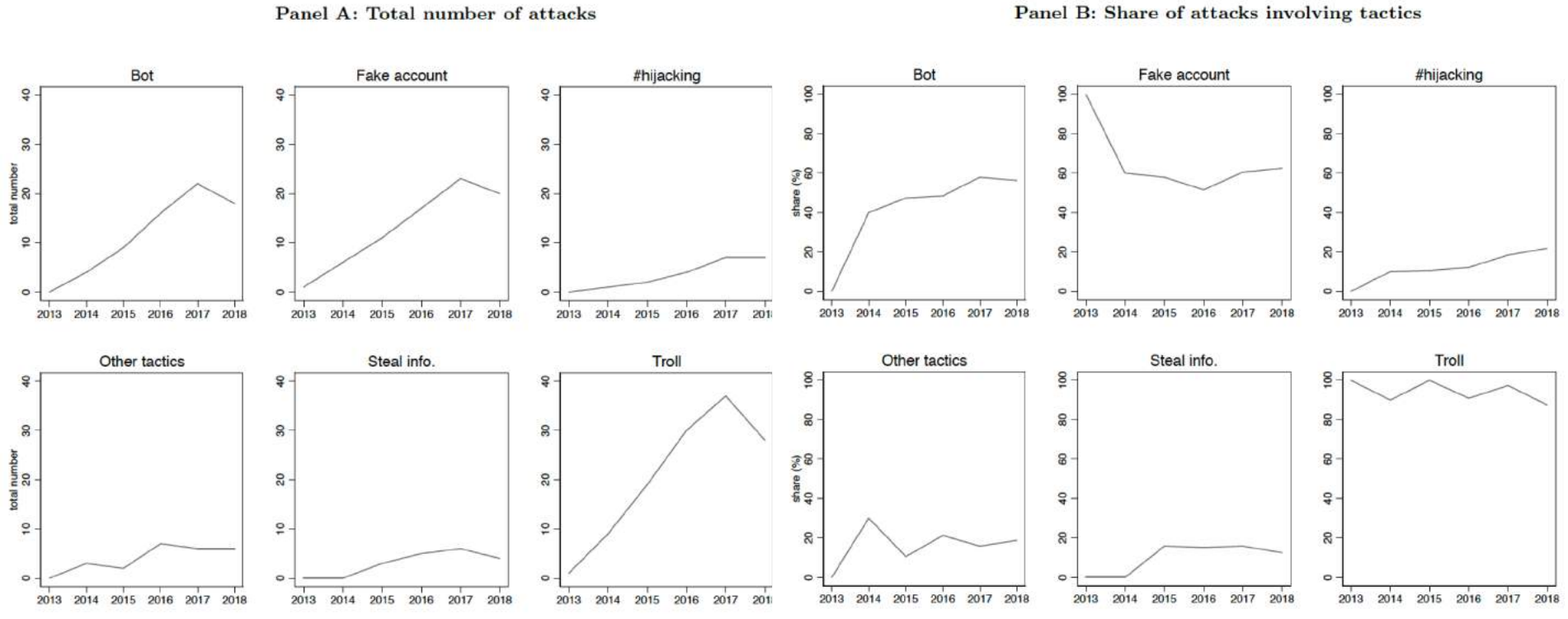




PRINCETON UNIVERSITY

Trends in Tactics

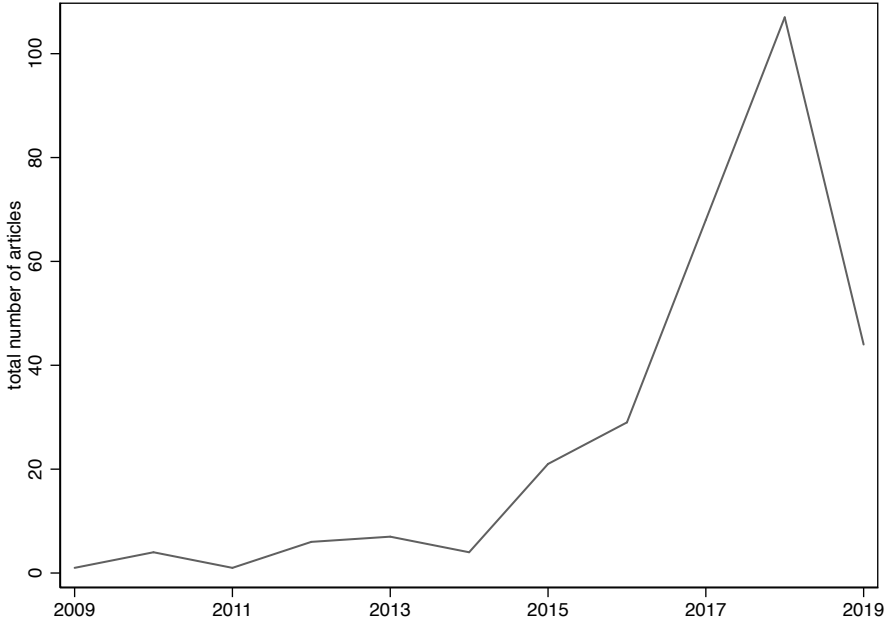
ESOC
Empirical Studies of Conflict

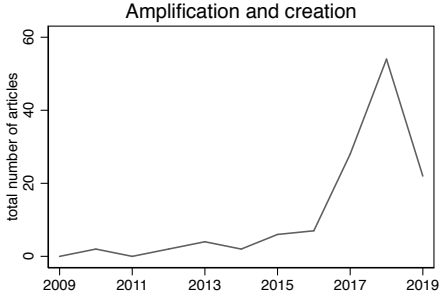


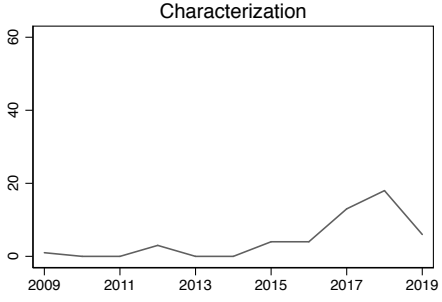
Policy Response by Targeted EU Countries

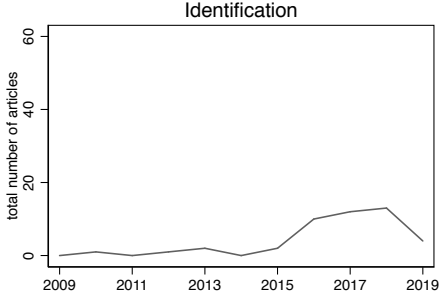
Country	Number of FIEs	Response on Election Security
UK	6	- Effort to help political parties to secure their systems. - NCSC established a “fake news unit”
Germany	3	- New military units to address information warfare - Legal reforms to give platforms 24 hours to remove designated types of content
France	3	- New laws around online content with emergency powers during election periods
Netherlands	3	- Shifted all elections to paper ballot
Austria	1	- No legal changes, though judges have enjoined specific content on Facebook
Italy	1	- New military command for cyber security - Civic education program and online paper for fake news
Poland	1	- New military command for cyber security

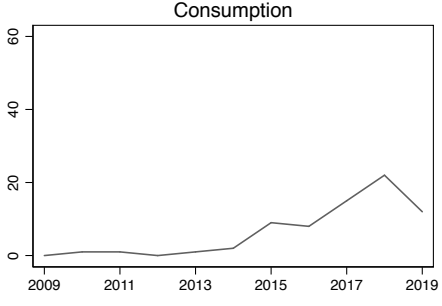
Research Attention (>326 articles to date)











PRINCETON UNIVERSITY

Remaining Hard Challenges

ESOC Empirical Studies of Conflict

- Observation on private services (e.g. Signal, WhatsApp)
- How content was spread after viewing
- Mechanisms through which promoted stories shape beliefs
- Impact of influence efforts on real-world political behavior