

# Defining Influence and Disinformation

**Olga Belogolova**

Policy Lead, Influence Operations





# A cacophony of terms

<b>Keywords</b>	<b>Number of Returned Articles</b>
Fake News	138
Misinformation	119
Propaganda	115
Disinformation	115
Influence Campaign	83
Influence Operations	45
Information Operations	15
Information War	10

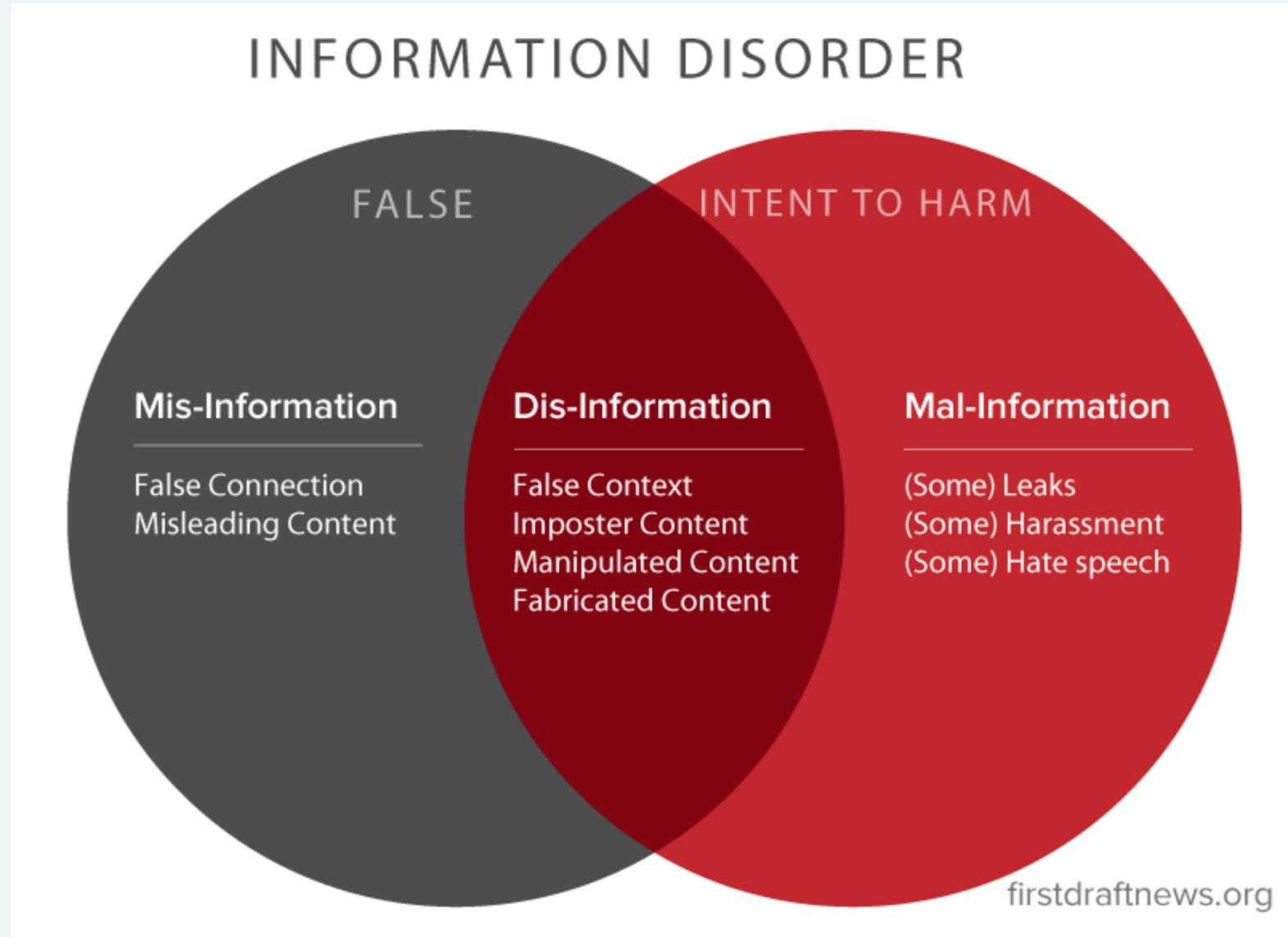
**Figure 1:** Number of returned articles mentioning keywords as searched on 15 July 2019 via the *New York Times* landing page featuring articles on “Russian Hacking and Influence in the U.S. Election”

# Disinformation



Source: "Captain of the Soviet Country Leads Us From One Victory to Another," Boris Efimov, 1933

# Misinformation and “MDM”



# Content based terminology



Source: First Draft News

# Content Responses to Content Problems



**Remove**

content and accounts  
that violate our  
Community Standards



**Reduce**

distribution of low quality  
content (including false  
news)



**Inform**

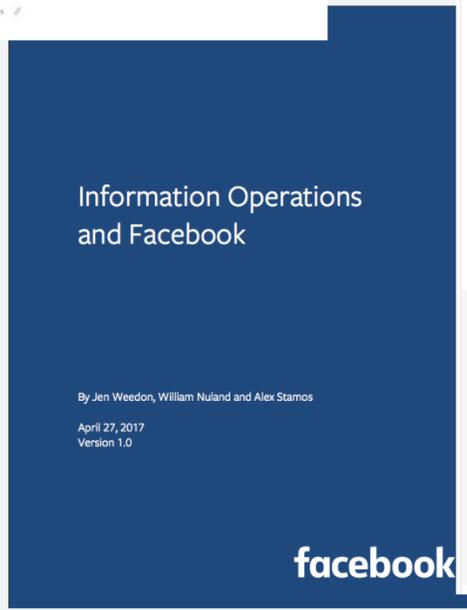
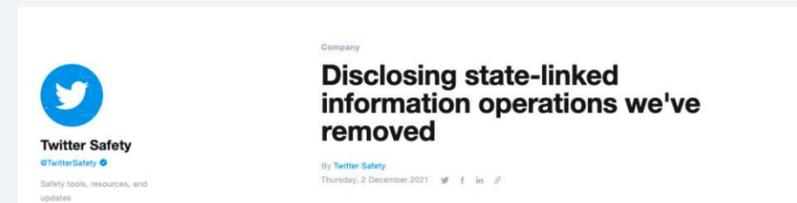
people by giving them  
more context, so they can  
decide what to read, trust,  
and share

# Information Operations

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)						
Core, Supporting, Related Information Activities	Activities	Audience/Target	Objective	Information Quality	Primary Planning/Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPEX)/Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electromagnetic Spectrum	Security	JOPEX/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPEX/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPEX/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security		
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance		
Military Deception	Military Deception	Cognitive	Mislead	Accuracy		
Operations Security	Operations Security	Cognitive	Deny	Security		
Supporting Capabilities	Information Assurance	Informational	Protect Information and Information Systems	Security		
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability		
	Physical Attack	Physical	Destroy, Disrupt	Usability		
	Counterintelligence	Cognitive	Mislead	Accuracy		
Related Capabilities	Combat Camera	Physical	Inform/Document	Usability, Accuracy		
	Civil Military Operations	Cognitive	Influence	Accuracy		
	Public Affairs	Cognitive	Inform	Accuracy		
	Public Diplomacy	Cognitive	Inform	Accuracy		

Source: JP 3-13

Figure I-3. Information Operations Integration into Joint Operations



**Nathaniel Gleicher** @ngleicher · Jan 9  
What underlies your desire to describe based on the activity (info) v the goal (influence)? And actually, isn't it reasonable to say that influence is both the goal (the noun form) and the activity (the verb form)?

**Yoel Roth** @yoyoel · Jan 9  
Decidedly NOT the verb form! That presumed the activity is successful - which is an empirical question that needs to be answered (and which we generally overestimate, I think). But that's a separate issue.

**Nathaniel Gleicher** @ngleicher · Jan 9  
Hmmm. Saying they're attempting to influence doesn't grant that they are successful. And I agree it shouldn't — public debate 100% overestimates the impact of IO. But I see the risk there — that's definitely a trap to avoid.

**Nathaniel Gleicher** @ngleicher · Jan 9  
As we discuss this, I think I prefer "influence" b/c it defines IO by the actions of threat actors, as opposed to their payload. And the payloads are often unremarkable. Overemphasis/analysis of/ fascination with IO payload is a recurring problem.

**Alicia Wanless** @lageneralista · Jan 9  
I can see @yoyoel and Twitter's point on that. And it also highlights the challenges of definitions being universally applicable. What might work for policy in one context might not make sense elsewhere. Lately I've been leaning towards terms borrowed from ecology...

# Historical Terms: Political Warfare and "Active Measures"

**TOP SECRET** CS 11396

THE JOINT CHIEFS OF STAFF  
WASHINGTON 25, D. C.

23 May 1944

MEMORANDUM FOR THE DIRECTOR OF STRATEGIC SERVICES

Subject: Outline Plan for Political Warfare -  
"OVERLORD"

Reference: JCS memorandum to OSS, dtd 23 May 44,  
subject as above

Enclosure: CCS 545/5, 22 May 44, subject as above,  
copy #65

Supplementing above reference, the enclosure is  
furnished herewith for your information and files.

*OCOL J. GRIDLEY*  
Colonel, G.S.C.  
Assistant Secretary

Approved For Release 2001/03/04 : CIA-RDP79S01457A000200010004-3

~~SECRET~~  
CONFIDENTIAL

20 June 1955

MEMORANDUM FOR: DEPUTY DIRECTOR OF INTELLIGENCE

SUBJECT: Mr. Burnham's Speech on Political Warfare,  
Including Propaganda

Mr. Burnham included in his definition of political warfare  
practically all forms of warfare short of open use of force--  
economic warfare, psychological warfare, etc.

The gist of his remarks was that the U.S. had no overall  
plan and no overall objective for the conduct of political war-  
fare, and as a result little had been accomplished although much  
money had been spent. He advocated preparation of an overall  
plan, the assignment of specific missions, and the organization  
of task forces to accomplish them; e.g., a task force to separate  
Albania from the Bloc by a certain date.

His speech was well prepared, clever, and well delivered,  
with many colorful phrases. He was roundly applauded. My own  
impression was that he disregarded entirely the probable conse-

TOP SECRET

April 30, 1948

COPY... OF... COPIES

**THE PROBLEM**  
The inauguration of organized political warfare.

**ANALYSIS**

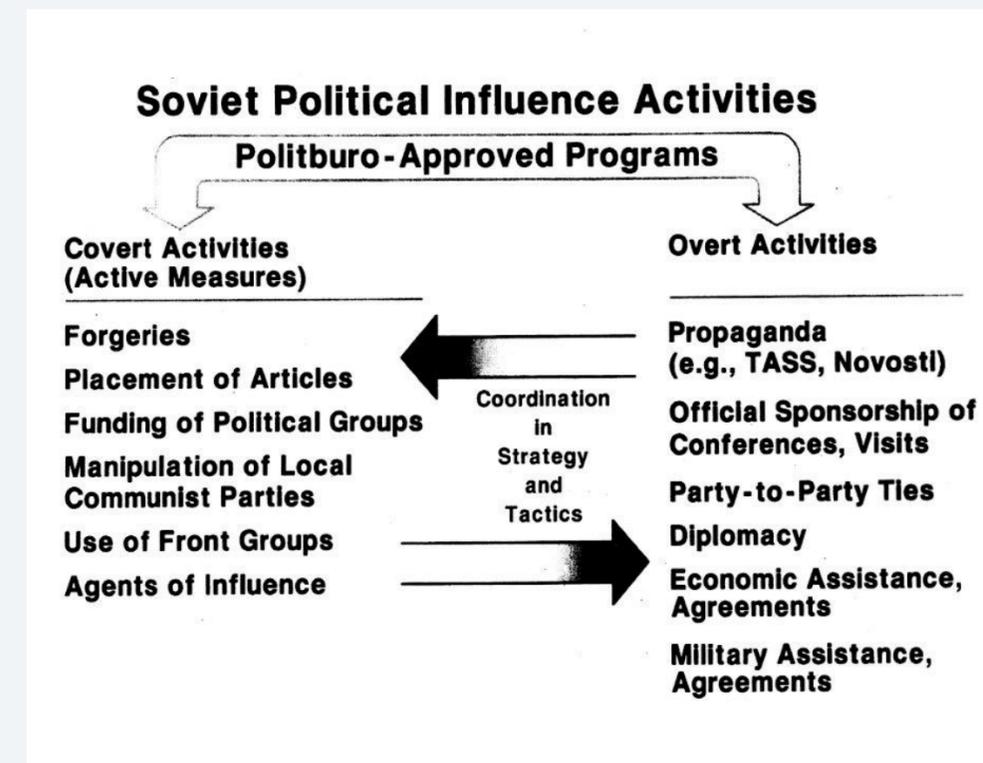
1. Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives, ~~to further its influence and authority and to weaken those of its adversaries.~~ Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.
2. The creation, success, and survival of the British Empire has been due in part to the British

\*\*\*\*\*

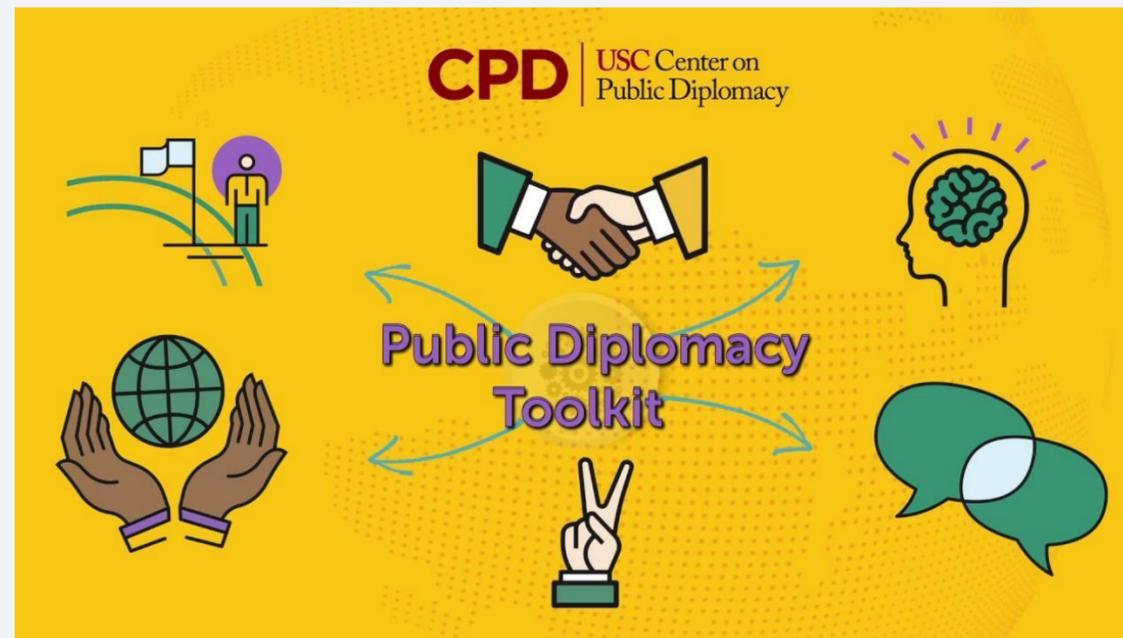
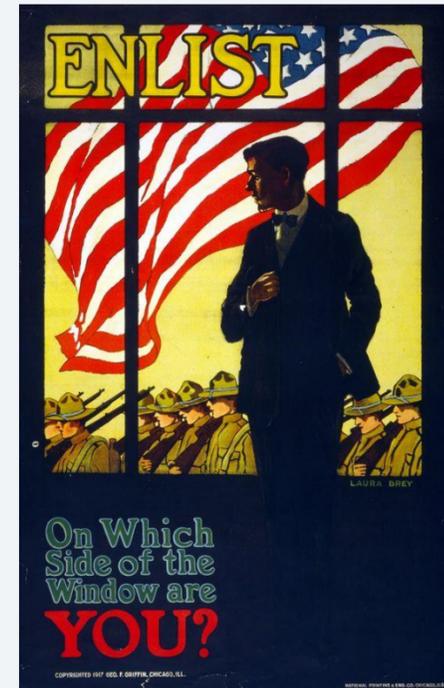
**ACTIVE  
MEASURES**

The Secret  
History of  
Disinformation  
and Political  
Warfare

Thomas Rid



# Propaganda and Public Diplomacy



# Influence Operations

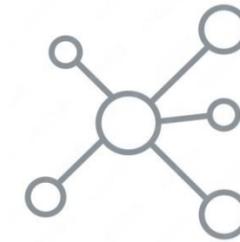
## Influence Operation (IO)

Coordinated efforts to manipulate or corrupt public debate for a strategic goal.



### Overt IO

State media, official government actors, etc.



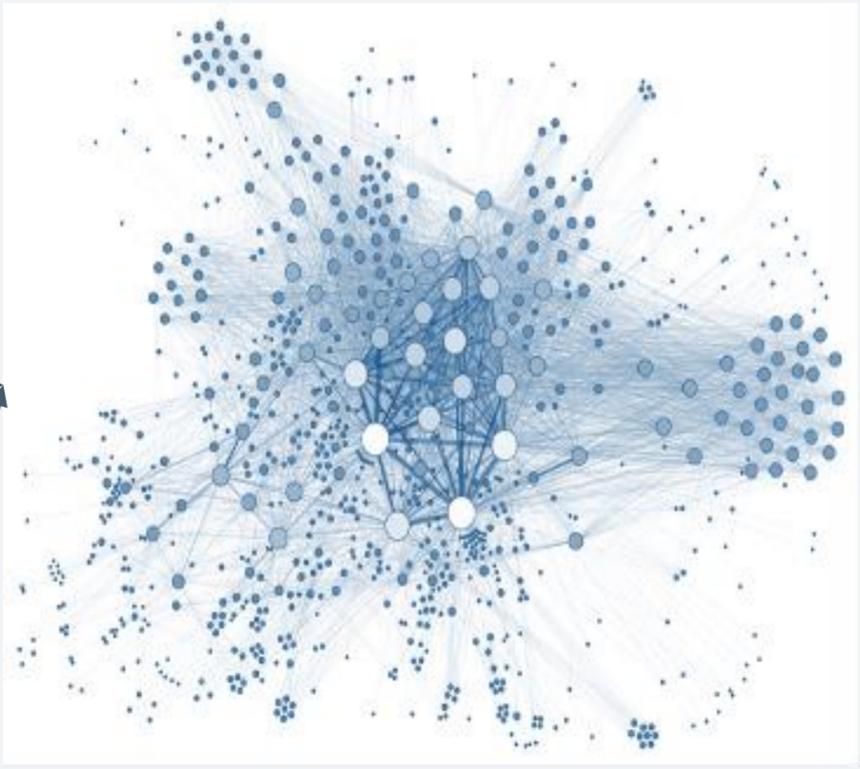
### Covert IO

Coordinated Inauthentic Behavior, foreign Interference

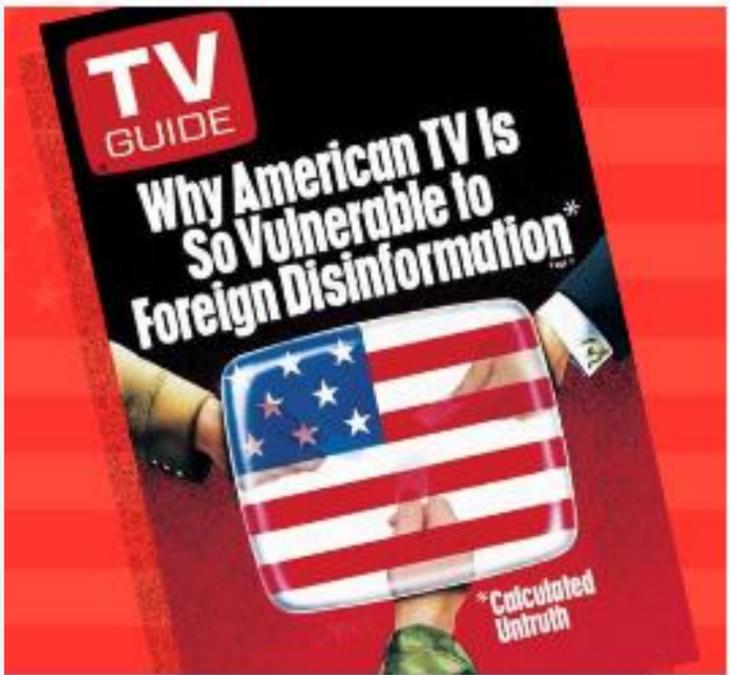
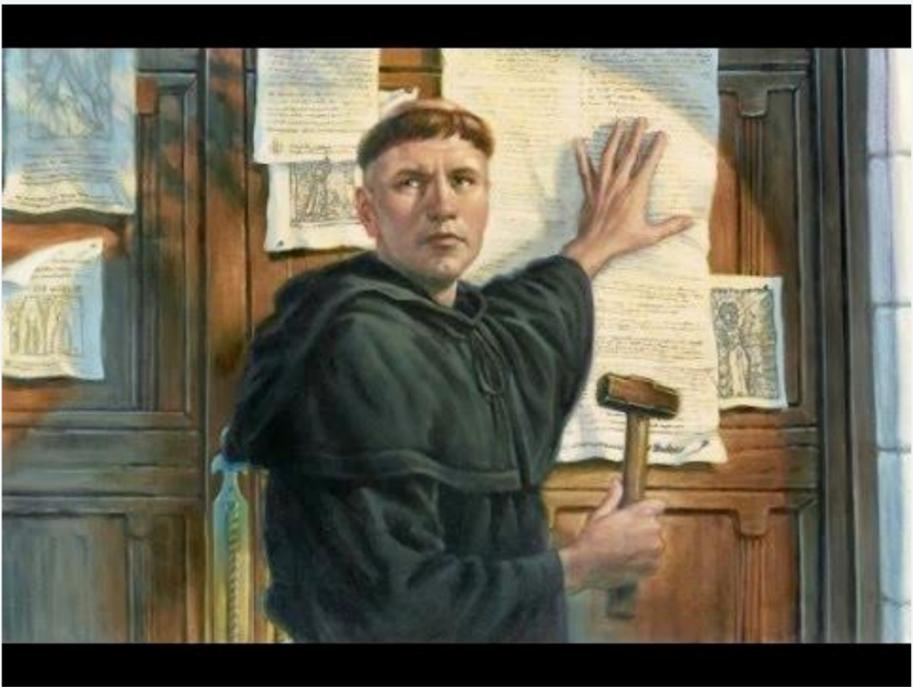
Global CIB disruptions, 2017-2021  
(by country of origin)



How did we go from influence ops to CIB?



# A long trail of deception and influence



# Deterrence in the IO space

## de·ter·rence

/də'tərəns/

noun

the action of discouraging an action or event through instilling doubt or fear of the consequences.

**Disruption** (removal of networks / fake accts, blocking domains)

**PNG** (persona non grata)

**Disclosure** (public sharing of threat research and analysis, including attribution when possible)

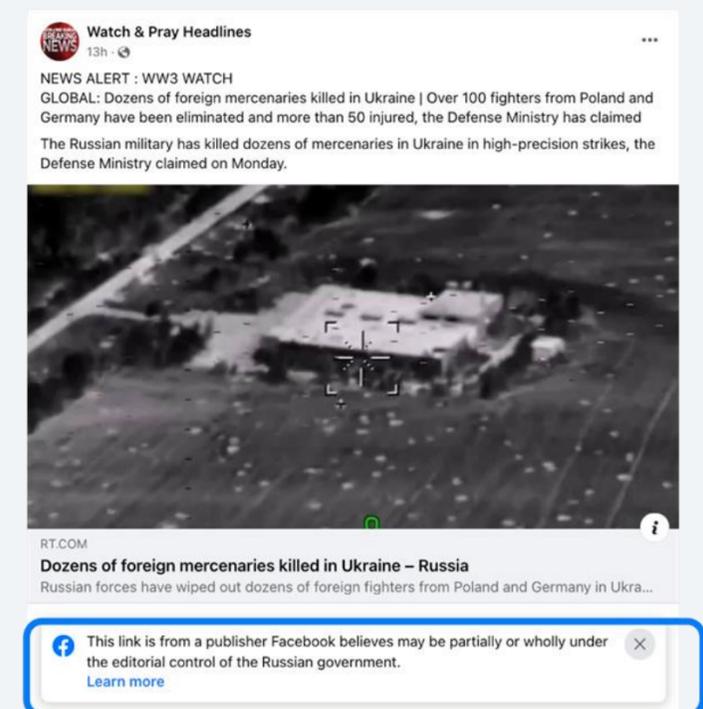
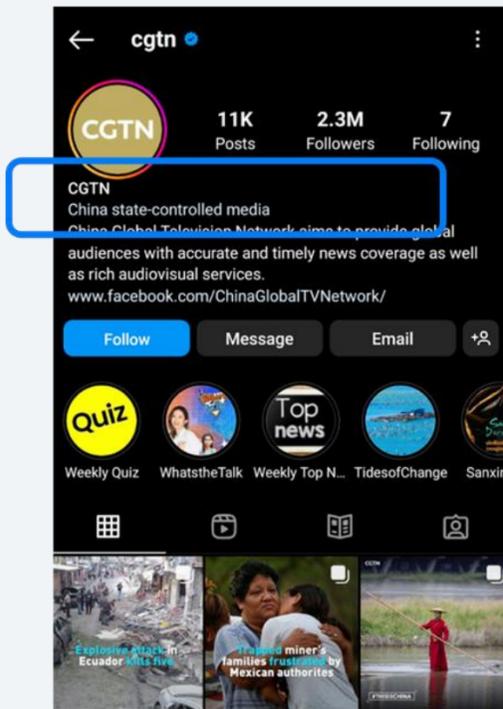
**Transparency** (labels, informational notifications)

**Notification** (User alerts)

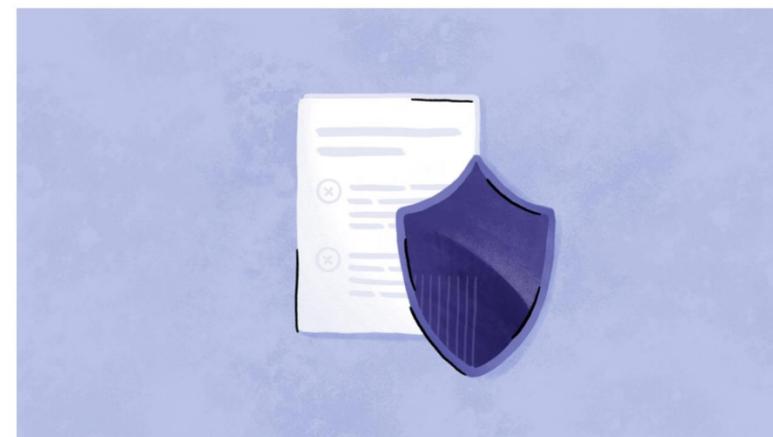
**Information sharing** (industry, government, civil society)

**Soft action to bring violators back in compliance** (demotion, warnings, etc.)

# Deterrence in the IO space



Meta  
**Removing Coordinated Inauthentic Behavior From China and Russia**  
September 27, 2022  
By Ben Nimmo, Global Threat Intelligence Lead and David Agranovich, Director, Threat Disruption



Meta  
**Banning Twinmark Media Enterprises in the Philippines from Facebook**  
January 10, 2019



# Signals of Success?

Threat actors forced into better opsec/adapt

Threat actors shift to use other platforms

Threat actors get caught before they can build an audience

Threat actors cannot get real-world traction

Civil society more aware of threat actor tactics

Increased whole-of-society lead sharing