



**SAFEGUARDING TRUTH**  
**UNDERSTANDING CYBER**  
**DISINFORMATION ATTACKS AND**  
**DEFENDING AGAINST THEM**

**Roy Zinman**

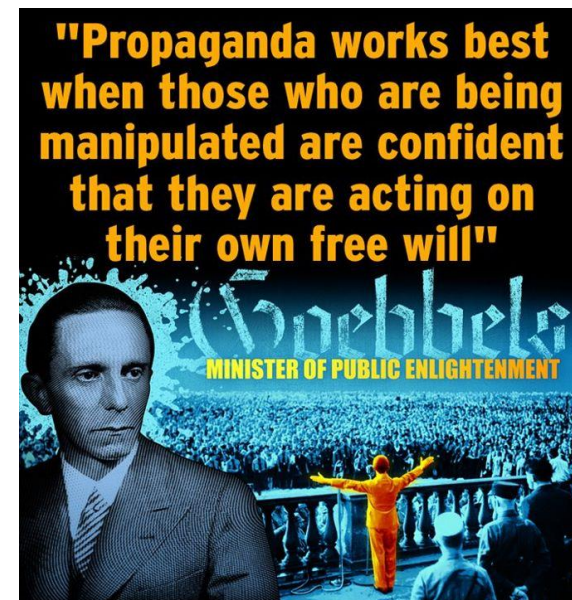
**Senior OSINT and Cybersecurity consultant, Israel**



# WHAT IS INFORMATION WARFARE ?

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

- ❑ **Information warfare** is the tactical and strategic use of **information** to gain an advantage
- ❑ Using information to mislead, subvert and paralyze the opponent
- ❑ Information Warfare existed throughout the ages
- ❑ The information age and social media made information warfare infinitely more potent, dangerous and effective:
  - ❑ Accurate intelligence
  - ❑ Powerful and fast dissemination
  - ❑ Immediate feedback cycle



State level strategic attack exposed



Other state and private actors  
imitate methods and tools



Everyday attacks

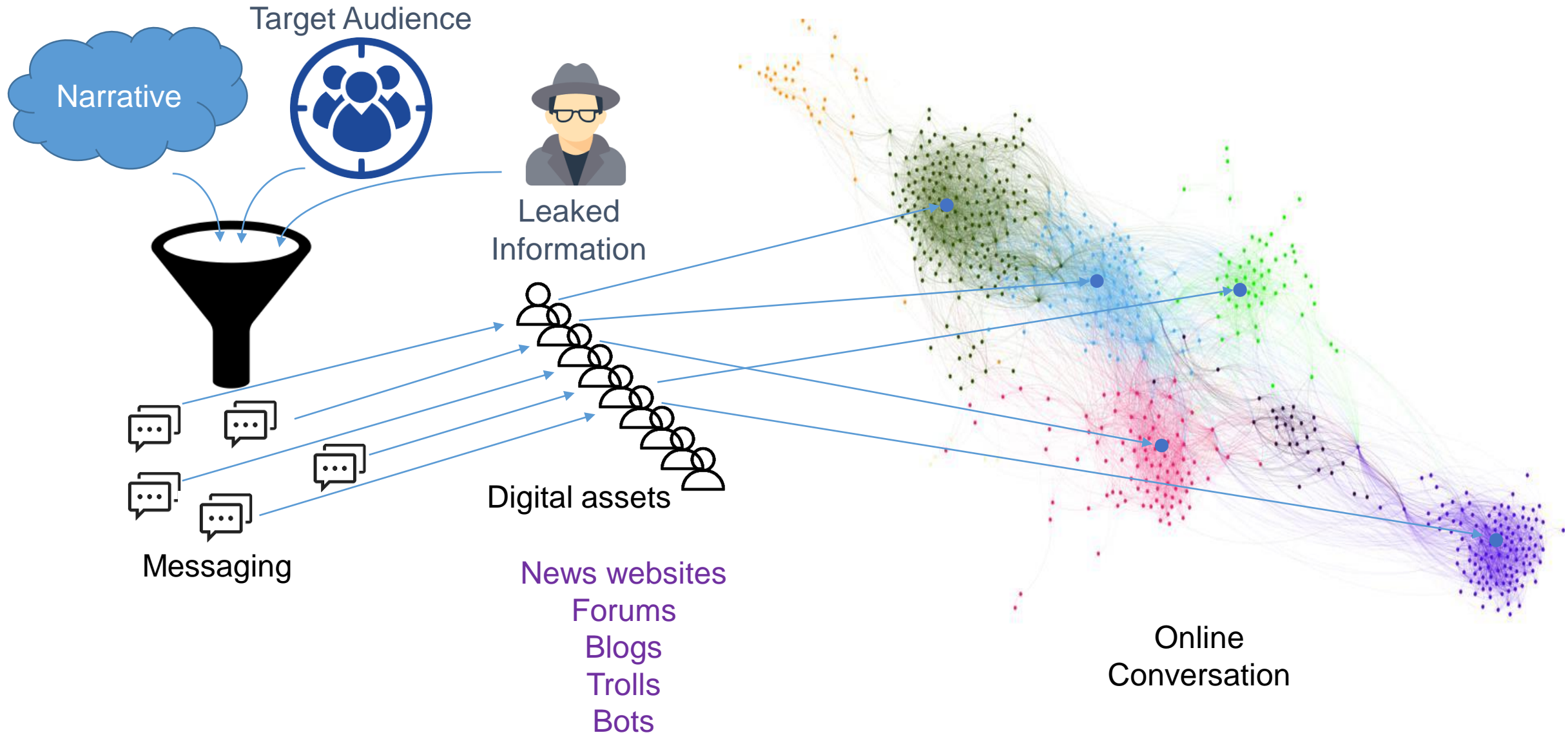




# INFORMATION WARFARE CAMPAIGN

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE





Israel



Iran



Pakistan



Moldova



Philippines



Saudi Arabia





- Combining tools and methods from state-sponsored arrays with influencer marketing technologies and know-how
- Affecting competitors by amplifying negative news
- Manipulating the price of traded stocks by leveraging sentiment – based trading algorithms
- Most affected verticals:

## Pharmaceuticals

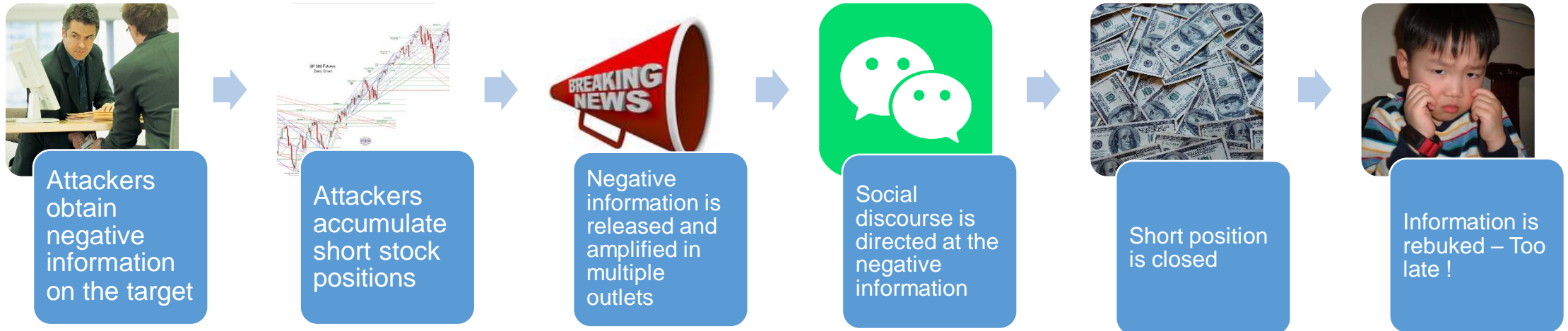


## Automotive



## Natural Resources

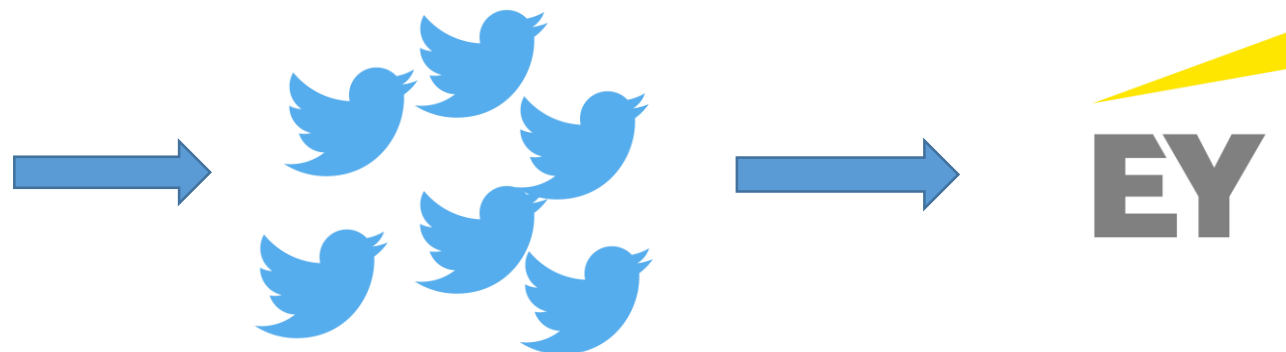






# AG WIRECARD - CASE STUDY

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE



Wirecard AG  
ETR: WDI

+ Follow

147.75 EUR +0.50 (0.34%) ↑

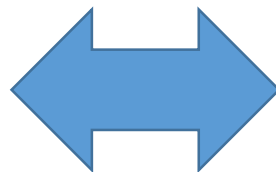
8 Aug, 16:45 GMT+2 · Disclaimer

1 day 5 days 1 month 6 months YTD 1 year 5 years Max



A raging war on twitter between supporters and short sellers

Abundant use of false identities, anonymous blogging, hashtags and memes





## 2019 BEIJING CYBER SECURITY CONFERENCE

## Tweet frequency correlates with major market events



It is not clear who is responsible for information warfare security

CISO ?

PR ?

Marketing ?

Authorities ?

Social Media  
Platforms ?

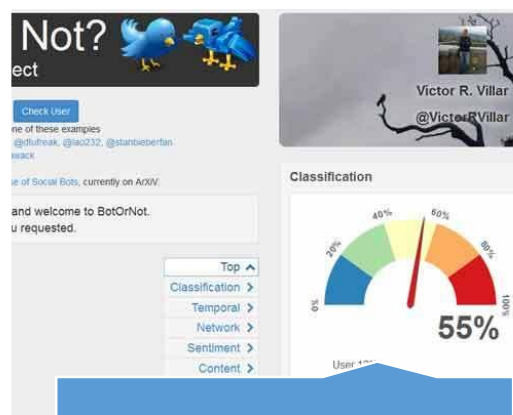
IW attacks are not perceived as cyber attacks

There are not enough solution with a clear ROI

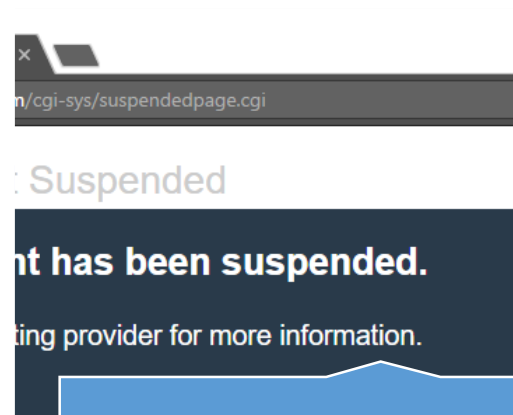




Monitoring



Detection



Mitigation



Incident Response

Monitor your brand and online assets in real time

Understand and monitor the threat actors

Follow IW attacks on competitors, industry members





Consider information leaks as potential attack vectors

Detect and identify the **adversary narrative**

Identify adversary media assets

Identify fake profiles promoting adversary narrative

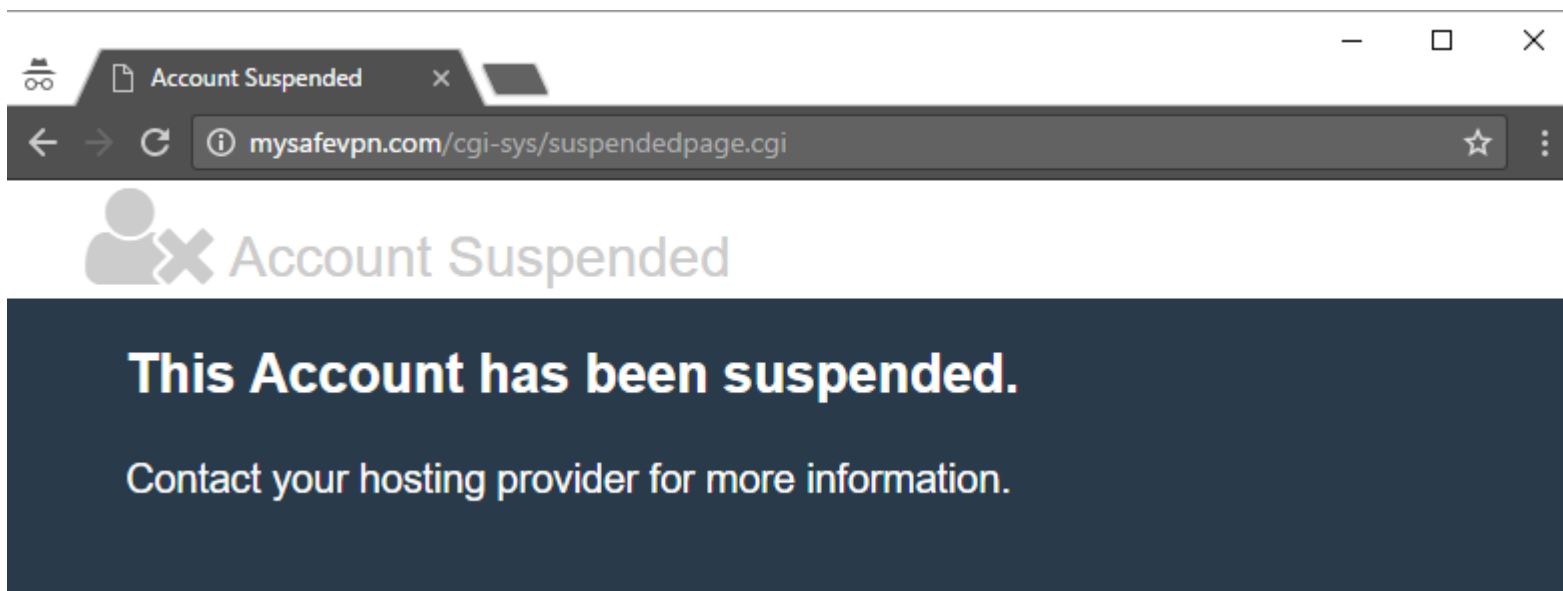
Create and keep a database of rival assets



Be transparent - Minimize exposure to leaks and damaging rumors

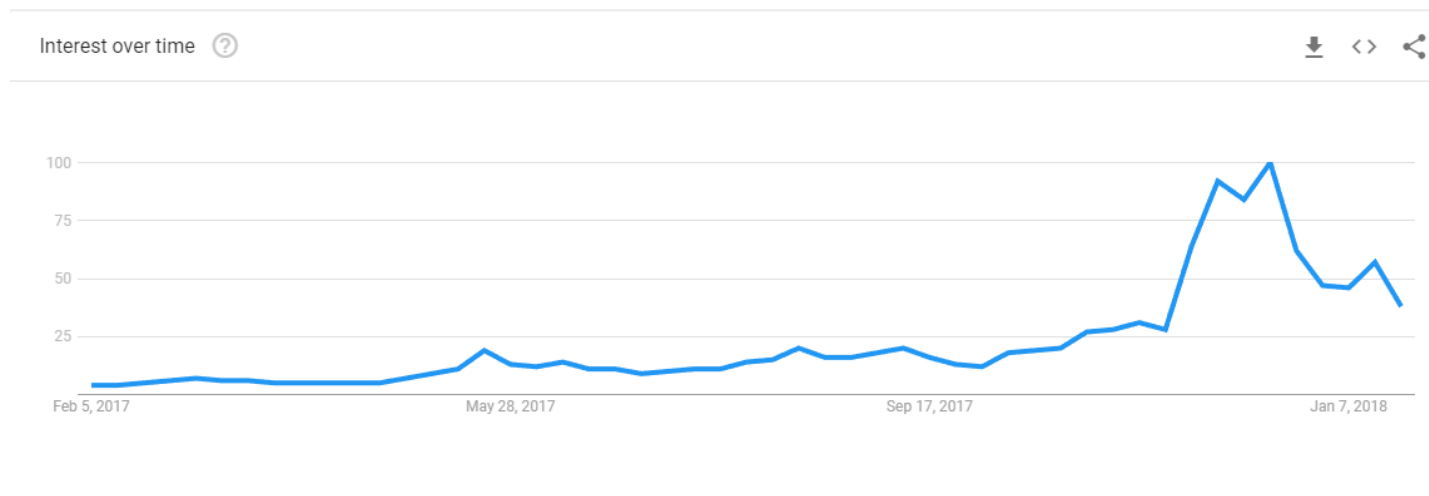
Prepare and maintain your own online assets and community

Prepare your counter – narratives






Rapid takedown of adversary assets  
Expose fakery and inauthentic behavior  
Disseminate counter-narrative with force



- ❑ Government and corporate organizations are exposed to IW attacks more than ever
- ❑ A carefully planned IW attack can be more damaging than any cyber attack, affecting stability, brand equity and stock prices
- ❑ Defending against IW requires a cybersecurity mindset, but also an understanding of social behavior, psychology and narrative
- ❑ Correct stance, tools and analysis can minimize the effect and even prevent dangerous IW attacks





The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE