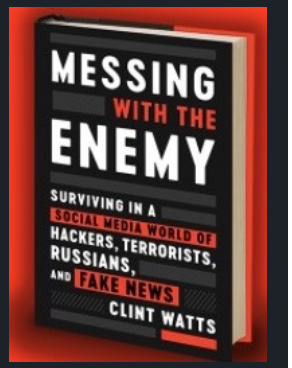
MIBURO

Messing With The Enemy

Surviving In A Cyber World Of Hackers and Trolls

Clint Watts

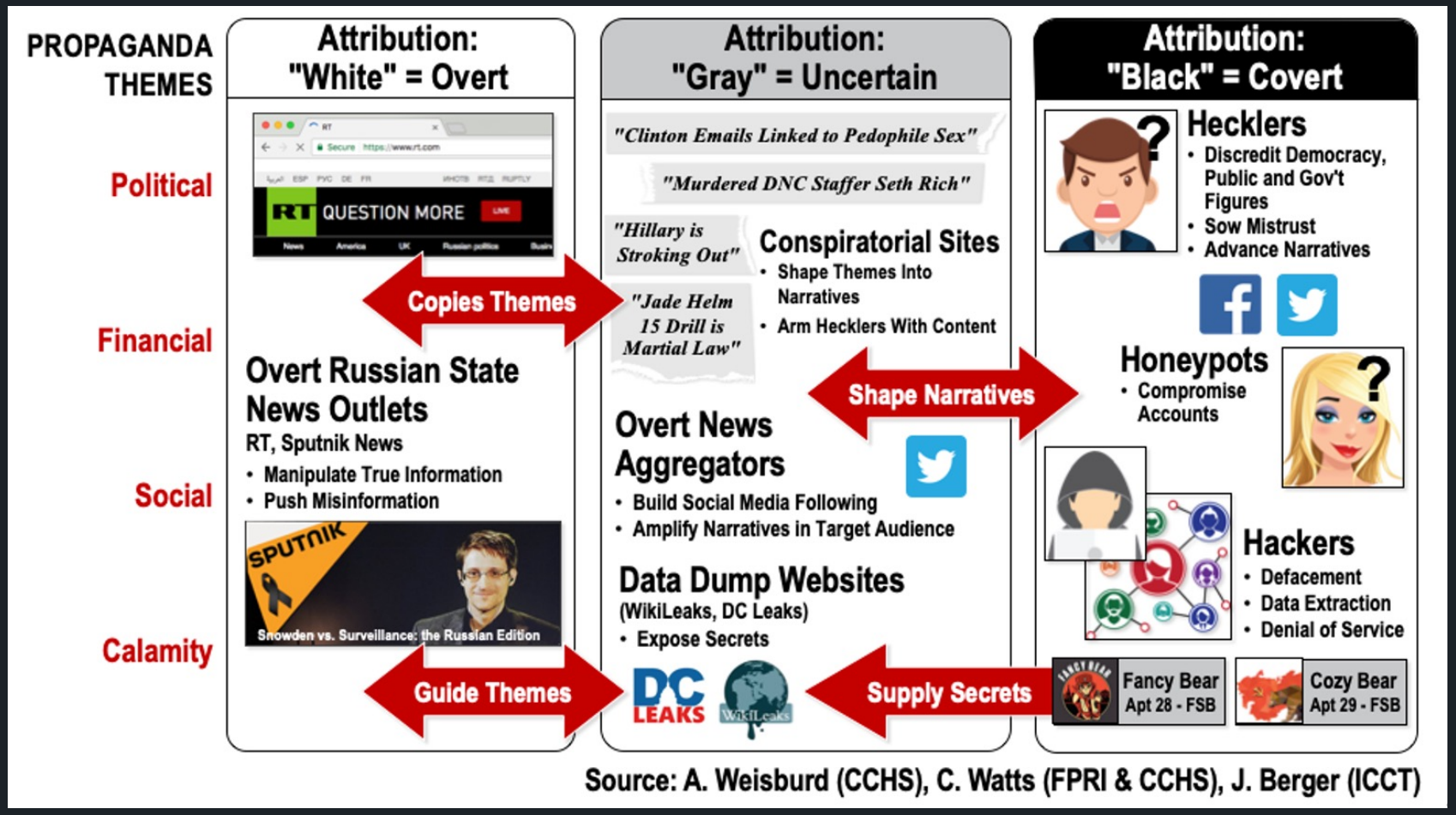
- Author of *Messing With The Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians and Fake News*
- Distinguished Research Fellow, Foreign Policy Research Institute
- Leader of the Miburo



MESA - JUNE 29, 2021

MIBURO

Full Spectrum Influence



Source: A. Weisburd (CCHS), C. Watts (FPRI & CCHS), J. Berger (ICCT)

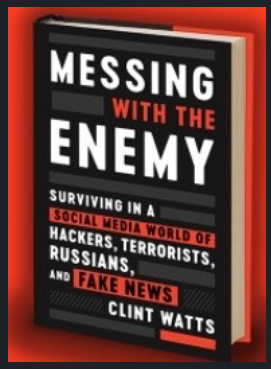
MIBURO

Preference Bubbles: 3 Dynamic Changes

Clickbait Populism – Promotion of popular content, opinions, and the personas that voice them

"The more a person plays to the crowd's preferences, the more they will be promoted, the more power they will accrue."

Clint Watts, *Messing With The Enemy,* May 2018

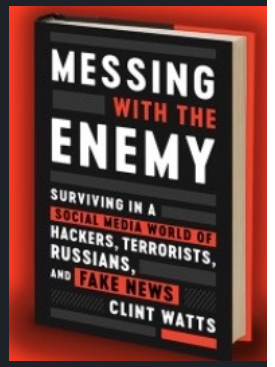


MIBURO

Preference Bubbles: 3 Dynamic Changes

- **Social Media Nationalism** – Collective adherence to a social media identity defined by shared beliefs demarcated by hashtags, avatars and account bios.

"Stronger allegiance to your digital tribe than your physical nation."



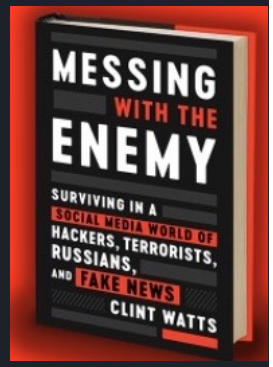
Clint Watts, *Messing With The Enemy,* May 2018

MIBURO

Preference Bubbles: 3 Dynamic Changes

- **Death of Expertise** – Belief that anyone connected to the Internet with a social media account knows as much as anyone else on any given topic, regardless of experience, training, education or specialty.

"Access to more information than ever, but we seem to understand less."



Clint Watts, *Messing With The Enemy,* May 2018

Why Does Social Media Lead Us To Believe Things That Are Not True?

3 Biases Affecting Social Media Perception

Confirmation

- *Tendency to interpret new evidence as confirmation of one's existing beliefs*

Implicit

- *Unconscious attitudes & stereotypes attributed to people without our conscious knowledge*

Availability

- *Assumption that most readily available information is accurate representation of reality*

SELECTED WISDOM

4 Things We Tend To Believe

First

- *That which we see first*

Most

- *That which we see most*

Trusted source

- *That which comes from a source we trust, whether the information is correct or not*

No rebuttal

- *Information not met by a rebuttal tends to be believed because there's no alternative explanation to consider*

Source: Clint Watts - https://clintwatts.substack.com/

Five Generations Of Online Manipulation – Evolution of Advanced Persistent Manipulators (APM)

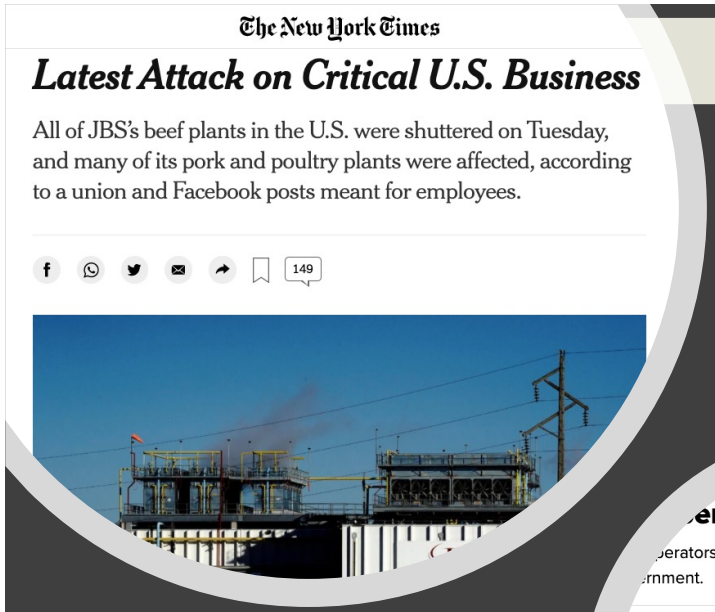
Generation	Era	Actors	Advancement
1	"Disrupt The System"	Hacktivists (Anonymous, Lulzsec, etc.)	• Hacking in pursuit of influence to shape public perceptions
2	"Exploit The System"	Extremists (AQ, AQ-Iraq, ISI, ISIS, IS)	• Full spectrum, multi-platform social media influence • Attempt at app creation
3	"Distort The System"	Nation States	• Widespread, strategic hacking for influence • Full spectrum social media influence • Disinformation Fusion Center - False personas, Fringe News Outlets, Integration of in-person Influence
4	"Dominate The System"	"Trolling-As-A-Service" (Cambridge Analytica, Others)	• Employment of artificial Intelligence • Advanced social bots • Creation of false audio/digital • In-person provocations • Migration to app influence
5	"Own The System"	Authoritarian Regimes (now) & Multi-National Corporations (future)	• Balkanization of the Internet driving users to apps • Incentivize human behavior to create preferred reality

Source: Clint Watts (Foreign Policy Research Institute & Alliance For Securing Democracy)

Advanced Persistent Manipulators (APM)

"Well resourced, Multi-platform, Full Spectrum"

Objectives	Methods	Actors
• **Influence Audiences** ➢ Shape Opinions ➢ Sell Products & Services • **Discredit Adversaries** • **Enlist Allies & Agents** • **Incite Fear & Provoke Conflict** ➢ Real or Imagined • **Distort Reality** ➢ Re-Write History ➢ Launder Reputations ➢ Alternative Explanation Flooding	Sophistication: *Less* → *More* • **Compromise Targets (Hackers)** • **Deploy Social Media Advancing Narratives** ➢ True & False, Overt & Covert • **Create Forgeries** • **Leverage Agents of Influence** • **Employ Computational Propaganda** • **Stage Real World Provocations** • **Create Alternative Information Outlets** • **Develop Pseudo-science, Revised Histories** ➢ Via Think Tanks, Non-Profits & Universities	Resources: *Less* → *More* • **Activist Groups** • **Extremist Groups** • **Nation States** • **Political Campaigns, PAC's** • **Lobbyists & Public Relations Firms** • **Extremely Wealthy**



Rise Of Ransomware

- Attacking All Industries In All Countries
- Spearphishing scaled by Ransomware development & deployment as a business model
- Digital Currencies For Criminal Gain (RansomWare)
- Governments trying to match the massive escalation in the problem

MIBURO

Preparing For Hackers & Trolls

- **Have a social media usage policy for employees**
- **User training for cyber security *& social media***
- **Maintain an insider threat program beyond just data loss**

Talent, Teamwork, Tradecraft & Technology

- ***Real time brand protection – speed is essential***
- ***Content development & dissemination***
- ***Tips & indicators system***
- ***Key network monitoring***

- **Develop & rehearse playbooks – Social Media & Hacking**
  - ***Respond to smear campaign***
  - ***Strategy for public engagement***
  - ***Know Your Leader, Execute your plan for containment, restoration, and information sharing***