NASS 2020 - Winter Conference
31 January 2020

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
• Non-Resident Fellow, Alliance For Securing Democracy, German Marshall Fund
“Social media tails in the virtual world wag our dog in the real world.”

Clint Watts, *Messing With The Enemy*, May 2018
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
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
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
### Five Generations Of Online Manipulation – Evolution of Advanced Persistent Manipulators (APM)

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

Source: Clint Watts (Foreign Policy Research Institute & Alliance For Securing Democracy)
### Advanced Persistent Manipulators (APM)

*Well resourced, Multi-platform, Full Spectrum*

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Methods</th>
<th>Actors</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Influence Audiences</td>
<td>• Compromise Targets</td>
<td>• Activist Groups</td>
</tr>
<tr>
<td>➢ Shape Opinions</td>
<td>• Deploy Social Media</td>
<td>• Extremist Groups</td>
</tr>
<tr>
<td>➢ Sell Products &amp; Services</td>
<td>• Advancing Narratives</td>
<td>• Nation States</td>
</tr>
<tr>
<td>• Discredit Adversaries</td>
<td>• Create Forgeries</td>
<td>• Political Campaigns, PAC’s</td>
</tr>
<tr>
<td>• Enlist Allies &amp; Agents</td>
<td>• Leverage Agents of Influence</td>
<td>• Lobbyists &amp; Public Relations Firms</td>
</tr>
<tr>
<td>• Incite Fear &amp; Provoke Conflict</td>
<td>• Employ Computational Propaganda</td>
<td>• Extremely Wealthy</td>
</tr>
<tr>
<td>➢ Real or Imagined</td>
<td>• Stage Real World Provocations</td>
<td>➢ Oligarchs, Celebrities, MNC Executives</td>
</tr>
<tr>
<td>• Distort Reality</td>
<td>• Create Alternative Information Outlets</td>
<td></td>
</tr>
<tr>
<td>➢ Re-Write History</td>
<td>• Develop Pseudo-science, Revised Histories</td>
<td></td>
</tr>
<tr>
<td>➢ Launder Reputations</td>
<td>➢ Via Think Tanks, Non-Profits &amp; Universities</td>
<td></td>
</tr>
<tr>
<td>➢ Alternative Explanation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>➢ Flooding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: C. Watts (Alliance For Securing Democracy & Foreign Policy Research Institute)
### Social Media Influence – Multi-platform, Full Spectrum

<table>
<thead>
<tr>
<th>Objective</th>
<th>Platforms</th>
<th>Purpose &amp; Advantages</th>
</tr>
</thead>
</table>
| **Placement** | **Primary:** 4Chan, Reddit  
**Secondary:** 8Chan, YouTube, Facebook |  
- Insert forgeries into social media discussions  
- Create & sow conspiracies in target audiences  
- Hide source of forgeries & attribution to Kremlin  
- Spread kompromat on targeted adversaries, both true & false information |
| **Propagation** | Twitter  
**Primary:** Facebook |  
- Spread narratives through overt accounts & covert personas  
- Amplify select target audience stories & preferable narratives supporting Kremlin goals *(Computational propaganda, make falsehoods appear more believable through repetition & volume)*  
- Inject stories into mainstream media worldwide  
- Attack political opponents, foreign policy experts & adversarial media personalities |
| **Saturation** | **Primary:** Facebook  
**Secondary:** Google Ads, LinkedIn, Instagram, Pinterest |  
- Amplify political & social divisions, erode faith in democracy through discussions & ads  
- Pull content from other platforms into trusted friends & family discussions  
- Recruit target audience for organic propaganda creation/distribution, or physical provocations (protests, rallies or even violence) |
| **Hosting** | YouTube |  
- Overt propaganda posts  
- Sharing of video content to target audience via producers & reporters rather than standard television channels |

Source: C. Watts (Foreign Policy Research Institute)
How Do We Survive In A Social Media World?

Countries
- Restore trust and confidence in institutions
- Reinforce data and science
- Refute falsehoods levied against the government
- Partner with social media companies to stop false information impacting public safety
- Information rating systems
- Anticipate breaches & smear campaigns

Companies & Agencies
- Have a social media usage policy for employees
- User training for cyber security
- Maintain an insider threat program
- Brand & reputational protection plan
  - Respond to smear campaign
  - Strategy for public social media engagement
How Do We Survive In A Social Media World?

**Citizens**

1. Determine the costs & benefits of social media use

2. Value human connections more than virtual connections

3. Spend more time in the physical world than the virtual world

4. Know the source of the information you consume

5. Listen more than you speak, Read more than you write, Watch more than you film

6. Understand what you will tend to believe

7. Know when you are an expert and when you are not an expert
Protecting Election 2020 From Foreign Interference

FPRI – #FIE2020 (www.fpri.org)
Foreign Influence Election 2020

IRAN MENTIONS OF 2020 PRESIDENTIAL CANDIDATES

LARGEST INCREASE IN MENTIONS

DECISION POINT: “Hack” or “Don’t Hack” to Power Electoral Inference

CONSTRAINTS

- Limited number of hackers available
- Limited amount of time to hack, aggregate and release stolen materials
- Hacking could be viewed as an act of war reciprocating retaliation

Top 10 Accounts by Tweets

- RT en Español
- Sputnik Türkiye
- Sputnik
- RT
- Sputnik France
- Telegram
- Sputnik Deutschland

Top 10 Accounts by Likes

- RT en Español
- Sputnik Türkiye
- RT
- Sputnik Deutschland
- Telegram
- Sputnik
- RT

Alliance For Securing Democracy – Hamilton 68 Dashboard

Hamilton 2.0 Dashboard

Top 10 Accounts by Retweets

- RT en Español
- Telegram
- Sputnik Türkiye
- Sputnik Deutschland
- RT
- Telegram
- Sputnik
- RT