Notes from the Lunch & Learn Forum
Muddied Waters: Disinformation and Propaganda in the Digital Age
January 10, 2018

Speakers:
Matt Chessen, Senior Technology Policy Advisor, E/STAS
Will Stevens, Director of Public Diplomacy Tradecraft, FSI
Tonia Weik, Senior Advisor for Strategic Communications, EUR/PD
Adele Ruppe, Chief of Staff, Global Engagement Center

CHANGES IN TECHNOLOGY

Computational propaganda is the use of technology (social media, big data, trolls, bots, etc.) to persuade, manipulate, inform, or disinform audiences. It can be legit. It can be malicious. It involves fake accounts that look like their target audience. Some are machines, some are real humans.

Bots are machines that release info on a schedule or respond to a trigger, such as a news alert or a tweet from a politician. They work well with Twitter. Types of bots include:

- Propaganda bots –They get info out.
- Follower bots – They "like" content, manipulating algorithms to generate trending topics.
- Road block bots – They spam #hashtags with garbage to bury, discredit, muddy the waters, etc.

Bots also engage in doxing, the unauthorized release of someone's personal information, such as their address or where their children go to school. Once that information is released, bots can be used to intimidate the target by piling on threats.

Bots can be used to create a mob mentality, swapping legitimate expertise for the opinion of the mob. For example, a genuine expert writing on a topic gets multiple bot-driven comments attacking their opinion or them personally. This will lower readers' opinion of the expert.

Some of these activities aren't necessarily illegal, although they often violate terms of service.

When we speak about AI developments in computational propaganda, we're talking about "Narrow AI," not Skynet. Regardless, narrow AI is capable of:

- Life-like chat bots, such as Zo. If you didn't know better, you'd think it's a person.
- Dynamic content creation. They can compose music, text, and generate fake news videos.

- Affective computing. It can notice and express emotions via text, audio, and video.
- AB testing. It can fine tune messages.
- Audio and video manipulation. It can create convincing fake audio/video.
- Psychometric profiling. There are 2,000-3,000 pieces of data available on each person in America, collected from the things we share online and on social media in particular. This data can be mined to hyper-target individuals and audiences.

These technologies have digital economies of scale. If you can make one, you can make many. Plus, they never sleep. They're 24/7. That's why it doesn't work for one person to take on a bot army. It takes a broader strategy.

COUNTERING DISINFORMATION STRATEGIES

Disinformation campaigns focus on social divisions that already exist in a target country. They work when they fall on fertile ground. There are three priorities in combatting disinformation campaigns:

1. Work with partners. Build their capacities. Learn from them.
2. Promote truthful narratives. They must be proactive and targeted.
3. Build audience resilience through traditional PD tools.

Yes, the bots are scary. But social media also give us tremendous amounts of metrics and good data. We should understand those metrics, and we should use them.

We are suffering from information disorder, the nonstop avalanche of legitimate information, mixed with dis-, mis-, and mal-information, from a vast array of sources. It's immeasurably difficult to sort through it all. This has created a tectonic shift in how people are influenced. It happened before with radio and TV, it's happening now with social media. That's why social media must be integrated in strategic communications, not handed to the intern.

PD professionals must understand the influence environment. The essence of PD is to understand, inform, and influence. We're good at the "inform" part. We must focus on the "understand" portion.

The first of the pillars of The PD Strategic Framework is 'audience.' That's the right focus. The audience is the landscape. You have to know where you're operating to be effective. PD can make that happen at post. Hire local consultants. Use your understanding of the influence environment to influence DC. Write cables, inform colleagues, speak to the interagency. Our job is to understand, figure out how to consume the data, synthesize it with what the mission is doing, and inform DC.

We aren't always the best voices for our own message. It just depends on your audience. Every post needs an in country network of validators that share common narratives and values.

We spend most of our resources on programming and activities. We should spend more on understanding what's going on, understanding our audience, understanding what worked. But there is little incentive to pursue these things because EERs talk about actions and activities. We aren't rewarded continuing a predecessor's program or sharing information. That should change.

THE GLOBAL ENGAGEMENT CENTER

The Countering Foreign Propaganda and Disinformation Act, co-authored by Senator Rob Portman (R-OH) and Senator Chris Murphy (D-CT), passed as part of the 2017 National Defense Authorization Act. It provided a legislative mandate for the GEC to lead, synchronize, and coordinate USG response to state and non-state propaganda and disinformation. State and DOD are finalizing a Memorandum of Understanding on how to work in this space together.

Historically, the GEC was the strategic communications center to counter terrorists. State actors were added because of an understanding that all disinformation is part of a broad problem set.

We must be smart and strategic. Must be whole of mission, must be whole of government. Furthermore, we cannot cover everything. We must focus on key vulnerabilities and opportunities.

FACTS ARE REAL – ENLIGHTENMENT VALUES AND FIGHTING "POST-TRUTH SOCIETY"

We are trying to convince people to do what we want them to do. We seek to influence opinions and change minds. We must not do this through corruption, coercion, or disinformation. That is the information doctrine of our adversaries. Yet we do need our own information doctrine, one that focuses on truth and the norms democratic discourse. We fight the "post-truth society" with an open society.

Our adversaries see open society as a threat. They're attacking the credibility of the internet. They muddy the waters because if truth is obscure, then power is all that matters. The post-truth society is an authoritarian society. That's why we must never use the term information warfare. They believe information is a function of power. We believe it's a function of truth. Don't play their game.

Facts are real. Truth is attainable. The Enlightenment is the project of pursuing truth through reason. It is the foundation of our constitution and of democratic civilization. We must fight for and through our belief in truth. That's why U.S. and democratic values resonate around the world in the first place.

That's why we shouldn't fight disinformation by inhibiting free speech online. The rights we enjoy offline should be enjoyed online. People around the world want those rights, and activists depend on anonymous communication to do their work free from fear. It's true that social media is technically a corporate platform. You sign up to their rules, to their terms of use. Regardless, whether it's technically a free speech issue, we should stand on the side of openness.

KNOWLEDGE MANAGEMENT AND FURTHER READING

What we know should be stored, categorized, transitionable. It should be in a central place. We should move from documents to data. Data can be mixed, remixed, analyzed, and accessed.

Follow cable traffic, work with INR/OPN for opinion research, and hire local consultants at post to increase your store of knowledge.

THINK TANKS & RESEARCH INSTITUTIONS

Atlantic Council's Digital Forensic Research Lab : https://medium.com/dfrlab

The European Values Think Tank: http://www.europeanvalues.net/

The Computational Propaganda Project, Oxford: http://comprop.oii.ox.ac.uk/

The Shorenstein Center, Harvard: https://shorensteincenter.org/

The Hamilton 68 Dashboard: http://securingdemocracy.gmfus.org/blog/2017/08/02/hamilton-68-new-tool-track-russian-disinformation-twitter

REPORTS, ARTICLES, AND REMARKS

The PD Strategic Framework:
https://usdos.sharepoint.com/sites/R/Documents/PD%20Strategic%20Framework/PD-Strategic-Framework.pdf

Can PD Survive the Internet?
https://www.state.gov/documents/organization/271028.pdf

Acting U/S Bruce Wharton, Remarks at Workshop on "Public Diplomacy in a Post-Truth Society"
https://www.state.gov/r/remarks/2017a/268592.htm

Information Disorder: Toward an interdisciplinary framework for research and policymaking
https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/

The MADCOM Future:
http://www.atlanticcouncil.org/publications/reports/the-madcom-future

Computational Propaganda Worldwide: Executive Summary:
http://comprop.oii.ox.ac.uk/publishing/working-papers/computational-propaganda-worldwide-executive-summary/

The Weaponization of Information: the Need for Cognitive Security, Rand:
https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

Weaponized Narrative is the New Battlespace, Brad Allenby:
http://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/

Weaponized Narrative White Paper, ASU Weaponized Narrative Initiative:
https://weaponizednarrative.asu.edu/publications/weaponized-narrative-new-battlespace-0

The Rise of the Weaponized AI Propaganda Machine, Scout AI:
https://scout.ai/story/the-rise-of-the-weaponized-ai-propaganda-machine

The Russian "Firehose of Falsehood" Propaganda Model
https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money:
http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf

How Russia Hacks Our Democracy, Matt Chessen:
https://medium.com/short-bytes/how-russia-hacks-our-democracy-2c5460596bc3

Why did Russian social media swarm the digital conversation about Catalan independence?
https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/?utm_term=.4a3c287c8b97