INTELLIGENCE & NATIONAL SECURITY SUMMIT

Combating Disinformation

Breakout Session

Overview

Each panelist shared their definition of disinformation and the work they do to counter it. News and social media are common platforms for adversaries to peddle false narratives, with each approach requiring a different counter. The panelists reflected upon lessons learned from Russia's interference in the 2016 elections and considered possible disinformation campaigns in 2020.

Summary

While definitions vary, disinformation is generally viewed as the deliberate spreading of false information. The most high-profile disinformation campaign in recent years was Russia's interference in the 2016 presidential election, in which it spread false and divisive narratives on social media that spread through traditional media and infiltrated political discourse. However, many other adversaries engage in disinformation, which often takes the form of concerted propaganda efforts. Government and industry, particularly traditional and new media outlets, seek to expose and counter disinformation to ensure that information being proliferated online and in the news is indeed true.

Panelists

- **Brett Horvath**, President, Guardians.ai
- **Suzanne Kelly**, Publisher and CEO, The Cipher Brief
- **Daniel Kimmage**, Principal Deputy Coordinator, Global Engagement Center, State Department
- **Sujit Raman**, Associate Deputy Attorney General, Department of Justice
- **Dr. Kathleen Hall Jamieson**, University of Pennsylvania, (moderator)

Key Takeaways:

- Tactics of disinformation are changing in the era of social media. Adversaries are 'building on truth' by introducing some facts to hook an audience, and then misleading them by surrounding each fact with false narratives.
- Adversaries each have a different approach. Russia spreads outright falsehoods, China peddles misleading narratives, and Al-Qaeda and ISIS promote distorted interpretations of religious texts.
- There is a distinction between misinformation and disinformation: Disinformation must be false and intended to mislead. Misinformation can happen by accident.
- Hacking is often linked with disinformation: Accurate information is revealed through hacking, and then a false narrative surrounding it is promoted.
- Tools like machine learning, artificial intelligence, and deep fakes will be more developed in 2020 than they were in 2016. Public officials are saying the 2020 election will be more secure than the 2016 vote, but it's important to prepare for adversaries to employ new disruptive techniques.
- Mainstream media covering disinformation campaigns can legitimize false messages. They have a profit incentive to cover a story first, but they should remain cognizant of the moral dimension and real-world impacts of publishing before all the information reported can be verified and thoroughly sourced.
- The Department of Justice has developed a disclosure policy dictating when the public must be informed of a disinformation threat. Before 2016, no such policy existed.
- The Information Access Fund supports investigative journalism outside the United States that identifies and contests foreign propaganda.

Recommendations

- Media outlets must establish policies for identifying and countering disinformation rather than rely on government to dictate a policy for them.
- Increase awareness of the issue: Studies show that if people know they are likely to be manipulated, they are more discerning about the information they choose to consume.
- Consume news from more than one source and seek context for isolated facts.
- Stop conceptualizing those who fall victim to disinformation as the gullible and/or ignorant 'other'; even savvy consumers of information can be affected by sophisticated, state-sponsored influence operations.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is the leading nonpartisan, nonprofit trade association for driving public-private partnerships to advance intelligence and national security priorities. A 501(c)(6) membership organization, INSA strives to identify, develop, and promote collaborative approaches to national security challenges. INSA has more than 160 organizations in its membership and enjoys extensive participation from leaders and senior executives in the public, private, and academic sectors. Learn more at www.INSAonline.org.