Disinformation – Дезинформация (Dezinformatsiya)

Aristedes Mahairas
Mikhail Dvilyanski

Disinformation is defined by Merriam-Webster as “false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth.” [1] The word disinformation did not appear in English dictionaries until the 1980s. Its origins, however, can be traced back as early as the 1920s when Russia began using the word in connection with a special disinformation office whose purpose was to disseminate “false information with the intention to deceive public opinion.” [2] Russia considered disinformation as a strategic weapon to be used in its overall Active Measures strategy. Active Measures, активные мероприятия, is a Soviet term for active intelligence operations for the purpose of influencing world events to achieve its geopolitical goals. [3] Major General Oleg Kalugin, retired KGB, considered disinformation as a critical component of the Active Measures strategy. Major General Kalugin described this as “the heart and soul of Soviet intelligence. Not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.” [4] To achieve these ends, many different methods were employed; such as, the creation of front organizations, the establishment of opposition parties, the support of criminal and terrorist organizations, and even the spread of disinformation through official and unofficial channels designed specifically to sow discord among the targeted audience.

1960S: OPERATION NEPTUNE

Operation Neptune was one such example. In this 1964 disinformation operation, the Czechoslovak secret service, working with the KGB, participated in the sinking and

Special Agent in Charge Aristedes Mahairas heads the New York (NY) Special Operations/ Cyber Division. He previously served as Legal Attaché, Athens; Joint Terrorism Task Force Supervisor; Section Chief, Strategic Operations Section-Counterterrorism Division; Chief of Staff to the Executive Assistant Director, National Security Branch. Prior to entry with the FBI, he served as a Police Officer in NY City and received a Bachelor of Arts degree in Political Science, Baruch College, and a Juris Doctor, NY Law School.

staged discovery of four chests of Nazi intelligence documents which had been forged and made to appear as if they had been under water since World War II. These documents were designed to discredit Western politicians by revealing names of former Nazi informants who were still being used as spies in Eastern Europe. Ladislav Bittman, the Czechoslovak agent who defected to the West in 1968, originally placed the documents in Cerne Jezero, the Black Lake, and later led the divers, who were part of a documentary team, to make the discovery. Bittman, who ran the operation stated, "It was the Cold War and the goal was to re-awaken interest and discredit West German politicians. Another goal was to have the statute of limitations for war criminals, which would have expired in 1965, extended. Following the extensive media coverage, the countries that suffered during WWII demanded that the statute be prolonged. Germany eventually extended it and then agreed that there be no limited time in which their war criminals could be tried." [5]

1970s: U.S.-EGYPTIAN RELATIONS

Another example of KGB active measures is the robust Soviet disinformation campaign against the U.S.–Egyptian relationship and the Camp David peace process in the late 1970's. The campaign focused on derailing the Middle East peace process and exacerbating tensions, attempting to undermine U.S. standing and influence in the region. The KGB demonstrated aggressive use of forgeries during the campaign, including a forged document purportedly from the office of the U.S. Secretary of State for the U.S. President, using language offensive to Egyptian President Anwar Sadat and other Arab leaders. This forgery was anonymously delivered to the Egyptian Embassy in Rome in 1977. Also in 1977, a series of forged letters purporting to be official U.S. Government documents were delivered

Mike Dvilyanski served in the FBI from 2005 until 2018, most recently as Supervisory Special Agent at the Cyber Branch at the FBI's New York office. In this role, Mike led an investigative team focused on state-sponsored computer intrusions against U.S. interests and was responsible for the development and implementation of a cyber incident response framework for the FBI's New York office. Previously, Mike served as Supervisory Special Agent in the Cyber Division at FBI Headquarters in Washington, D.C., where he oversaw investigations of state-sponsored cyber threats. In 2017, Mike returned to FBI Headquarters to help lead the FBI's efforts to combat election interference and foreign influence operations. Mike graduated from the FBI Academy in 2005 and was assigned to the New York Field Office of the FBI, where he investigated Counterintelligence and Cyber matters.

to numerous locations. The letters advocated a "change of government" in Egypt and criticized President Sadat's leadership. Finally, in 1979, a forged letter from the U.S. Ambassador to Egypt was published in a Syrian newspaper. The letter was critical of President Sadat and expressed the U.S. position of wanting to "get rid of him without hesitation." The breadth and duration of this active measures campaign clearly illustrates the importance Soviet leadership placed on undermining US credibility and influence in the region as a key sponsor of the Camp David peace process. [6]

RECENT EVENTS

Nearly 100 years after Russia established its special disinformation office, an analysis of recent events shows that such disinformation campaigns no longer require the sole services of intelligence operatives of old. In fact, with the leveraging of technology and the use of both overt and covert methods, such disinformation campaigns can have an even greater impact to a wider audience in a rather short period of time. It should be noted however that the purpose of such campaigns remains the same. The goal is to create discord and confusion, and amplify existing divisive issues in order to further expand the space separating the targeted audience; thereby, making reconciliation between any two sides of a divisive issue even more difficult to achieve.

2016: LISA CASE

One clear example of this activity, utilizing both overt and covert channels to propel a disinformation campaign, is evidenced in the Lisa case which takes place in Germany. For two weeks in January 2016, the media focused on Lisa, a 13-year old Russian/German girl, who had gone missing for 30 hours and was reported to have been raped by Arab migrants. [7] The German police, as with any allegation of a serious crime, quickly investigated this matter, and in very short order, determined the story to be false. In fact, Lisa herself admitted to having been with friends during the time in question.[8] Despite the speed in which the German authorities were able to reach a logical conclusion, the story had taken on a life of its own.

SUCCESSFUL ALIGNMENT WITH SOCIAL MEDIA TO ACHIEVE DISINFORMATION

The Lisa saga began taking shape with Russia's state-sponsored Channel One which broadcasts into Germany in Russian. The story was then picked up by Russia Today (RT); RT Deutsch, and Sputnik. All three are well-known – overt – Russian government controlled media outlets. In fact, in 2017, RT and Sputnik registered with the U.S. Department of Justice under the Foreign Agents Registration Act (FARA) declaring their respective organizations as agents of a foreign power, to wit, Russia. This overt media activity was coupled with the covert actions of a Facebook group and anti-refugee website called Ayslterror, which was later determined to have links to Russia.[9] The actions of this group spurred various social media and rightwing groups to widely distribute the information on the internet, to include demonstrations which were organized via Facebook involving representatives of the German-Russian minority (Deutschlandrussen) as well as neo-Nazi groups.[10] This disinformation campaign focused on exploiting the existing divide among Germans as it related to the Arab-migrant issues and some speculate it was orchestrated and directed in response to Germany's leading role in the Ukraine crisis and Chancellor Merkel's subsequent stance on sanctions against Russia.

Whether it is the use of intelligence operatives in the field or intelligence operatives behind the keyboard, Russia has fully embraced a strategy of information warfare, one designed to achieve long-standing intelligence objectives in support of their overall geopolitical agenda. The Lisa case is one of a handful of cases that can be viewed as evidence that the Kremlin is engaged in a structured approach to leverage new age technologies.[11] [12] [13] A thoughtful analysis of the methodologies employed reveals an organized model that serves as a framework for conducting foreign influence operations in the Information Age, and incorporates several logical steps to ensure maximum impact.

The influence campaign begins by identifying existing socially and politically divisive issues followed by the development of messaging themes to amplify these divisions along existing fault lines. The adversary then begins to establish the technical infrastructure and networks of influence, which will ultimately be used to publish and perpetuate the campaign. Simultaneously, affirmative efforts are undertaken to obtain and produce material that will yield the desired objective. Once the sought after information is obtained, through hacking, forgery, or "creative" content such as articles, blogs, or specifically designed news stories presenting false information, it is then published to the targeted audiences for public consumption.

At this stage of the campaign, the objective is to create confusion surrounding the true motivation behind the content and hide the origins and sponsorship by the foreign government. Subsequent to publication and consumption, the adversary will engage in a concerted effort to amplify the messaging. This intensification is powered by the modern information landscape and social media. Here, the adversary begins to achieve scale in order to sow discord, confusion, and doubt by saturating the information space and amplifying divisive issues that appeal to existing biases of the target audience.

The principle objective of this activity is to get unwitting audiences to engage with the influence content and disseminate it further within their own social networks, thus extending its reach. The effect of this total effort is ultimately analyzed by reviewing the impact on and engagement by the audience to assess the effectiveness of the influence campaign; this may undergo a period of fine-tuning to maximize its impact. The entire process and its ultimate success relies on the coordinated efforts of the numerous overt and covert actors who take part in the manufacture of stories and information designed to manipulate the masses.

Russia’s 2016 US Presidential election influence effort highlights just how this methodical approach is precisely implemented. Bill Priestap, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation stated, “Russia’s 2016 presidential election influence effort was its boldest to date in the United States. Moscow employed a multifaceted approach intended to undermine confidence in our democratic process … which included the weaponization of stolen cyber information, the use of Russia’s English-language state media as a strategic messaging platform, and the mobilization of social media bots and trolls to spread disinformation and amplify Russian messaging.” [14] This statement clearly highlights the use of overt and covert means to create multiple false narratives designed to work together to shape the perception of the target audience.

A key objective of modern influence operations is to make true facts harder to find and garner consensus. The goal is to not just to present an alternate version of reality, but rather to contaminate the information space with many such versions, some of them conflicting, to confuse the audience and erode its ability to think critically. It is about creating a sentiment that no news source or narrative can be trusted and providing fodder to the audience to connect with whichever storyline most appeals to its pre-existing biases. It is about diminishing our collective ability to find the truth and agree on it. The modern information landscape allows for this to be achieved rapidly and at scale, by delivering false narratives directly to the audience much more quickly and broadly than was ever possible before. Achieving this objective is made easier when nearly two-thirds of American adults are getting at least some of their news on social media and where the act of sharing a piece of content (such as a post, a news story, or a meme) within one’s own social network can often be more important than its veracity. [15]

If we are to avoid the toxic consequences of disinformation, we need to sharpen our sense of skepticism and ask pertinent questions about the veracity and motivation of what we view and share. We need to engage in transparency and expose this behavior, shining a spotlight on it whenever we can. Education of the threat and providing context to enable critical judgment will help mitigate this vulnerability. Otherwise, if we do not challenge the dissemination of falsehoods, we not only allow, but also invite ill-intentioned forces to continuously negatively influence us all.

NOTES

1. "Disinformation" Merriam-Webster.com, Merriam-Webster, n.d. Web, June 3, 2018.

2. Ladislav Bittman, "The KGB and Soviet Disinformation: An Insider's View," Pergamon-Brassey's, 1985.

3. Christopher Andrew and Vasili Mitrokhin, "The Mitrokhin Archive: The KGB in Europe and the West," Gardens Books, 2000.

4. Oleg Kalugin, CNN Interview, Archived at the Wayback Machine, 2007.

5. Ladislav Bittman, "The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare," Syracuse University Research Corporation, 1972.

6. United States Department of State, Special Report No. 88, "Soviet Active Measures: Forgery, Disinformation, Political Operations", 1981.

7. Stefan Meister, "The 'Lisa Case': Germany as a target of Russian disinformation," NATO Review, https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

8. Ibid.

9. Alina Polyakova and Spencer P. Boyer, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition," Foreign Policy at Brookings, 2018.

10. Stefan Meister, "The 'Lisa Case': Germany as a target of Russian disinformation," NATO Review, https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

11. Neil MacFarquhar, "A powerful Russian weapon: The spread of false stories," The New York Time, August 28, 2016, https://www.nytimes.com/2016/08/29/world/wurope/russia-sweeden-disinformation.html.

12. United States of America v. Internet Research Agency LLC et al., https://www.justice.gov/file/1035477/download.

13. Joseph Menn, "Exclusive: Russia used Facebook to try to spy on Macron campaign – sources," Reuters, July 27, 2017, https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1ACOEI.

14. Bill Priestap, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Statement Before the Senate Select Committee on Intelligence, Washington, D.C., June 21, 2017, https://www.fbi.gov/news/testimony/assessing-russian-activities-and-intentions-in-recent-elections.

15. http://www.pewresearch.org/fact-tank/2017/10/04/key-trends-in-social-and-digital-news-media/.