INTELLIGENCE BRIEFING

CYBER DEFENSE
INTELLIGENCE

CYBER Defense Briefing

CYBER DEFENCE INTELLIGENCE CENTER

June 2, 2020

DISINFORMATION CAMPAIGNS

SCOPE: This intelligence briefing affects all industry segments and organizations.

Prepared by the Cyber Defense Coalition Intelligence Center Analysis Team.

DISINFORMATION CAMPAIGNS

Disinformation campaigns originated in the Soviet Union during the Cold War. The word did not even exist in English language dictionaries until the 1980's. The word originates from the Russian word "Dezinformatsiya" which was a KGB propaganda directorate. The campaigns utilize false information, are intended to create division, and deceive the public for a foreign adversary to sway public opinion.

Over the past few years, there have been multiple disinformation campaigns run against the United States, with a sharp increase In 2020. The most well know campaign was the 2016 Presidential Election campaign which has been attributed to the Russian government. We have also seen campaigns run to create racial and political division. These campaigns have been attributed to alt-right and Homegrown Violent Extremists (HVE)'s.

The United States has been targeted due to its global prominence and influence on geopolitical issues. The US will continue to be a target and the organizations running the campaigns are leveraging social media platforms and news media to propagate the false information. The campaigns are taking advantage of base human emotions such as fear and greed to target biases and drive deep division in the populace.

CDI's Intelligence analysts believe that we will see a significant increase in the number and types of campaigns in 2020 as we approach the Presidential election. The topics that will be leveraged to create this division will involve some of the following topics:

- Media legitimacy
- Gun rights
- Racial issues
- Immigration
- Political Party alliances
- Abortion rights
- Voter fraud
- Pandemic response
- Religious Rights
- Police abuse
- Climate Changes and Environmental Platforms
- Educational Costs
- Financial divide

Additional topics where beliefs on either side are strong and create a passionate response from the audience or there is a strong fear of the outcome of topic are also good targets for disinformation campaigns.

KEY ACTORS

There are several groups which are using disinformation campaigns to influence their specific agendas.

Nation-State Actors

Funded by foreign governments, the Nation-State actors have the largest influence and most potential impact. They are motivated by geopolitical topics and have a primary mission of either reducing the United States global power and position or distracting the US government efforts from critical missions which may have a negative impact on their country. Nation State campaigns are very effective at using social media and planting stories in traditional news media to sow discord in the United States population. They also conduct sophisticated psychological operations (PSYOPS) which are meant to convey select information and indicators to audiences to influence their emotions, motives, and objective reasoning, and ultimately the specific behaviors of governments, organizations, groups, and individuals. These actors can be military groups within the foreign government or external organizations which are engaged to run the campaigns for the foreign government. This makes attribution of the campaign back to a specific government very difficult.

Hacktivists and Homegrown Violent Extremists (HVE's)

Hacktivists and HVE's have extreme ideological and political agendas and benefit from creating discord that drives a wedge between different groups, demographics, political parties or any naturally occurring division that already exists in the United States population. These groups have created their own news sources, websites and cable tv stations and also heavily rely on social media to run their campaigns. These groups are less funded than the Nation-State Actors but still have their own funding sources and are very effective at disseminating their messages. These groups are also leveraged by the Nation-State actors as a vehicle in their disinformation campaigns.

Cyber Criminals

Cybercriminals are motivated by making money. They run campaigns that drive consumers and citizens to engage in their schemes to increase the likelihood of success. The current pandemic has seen a significant increase in the number of cyber crime disinformation campaigns. These have materialized in the form of phishing campaigns, false cure campaigns, and financial bailout schemes that leverage disinformation to increase or leverage fear to cause targets to fall for their scams.

TYPES OF ATTACKS

The actors using disinformation utilize many different tools to run their campaigns.

Social Media

Platforms like Facebook, You-tube, Twitter, Instagram, and even LinkedIn have been heavily used to disseminate their information. These platforms are easy to use, free and are challenged with first amendment issues that make it difficult to block or remove the false information. The actors are able to post messages which have opposing points of view and by targeting both sides of an issue can rapidly increase the discord and drive the division.

Traditional Media

News media sources such as newspapers, broadcast media, and cable news stations are financially motivated to sell advertising and must have leading stories to attract media buyers. The shift to opinion-based news has also created an opening for disinformation to be spread. This rush to release news quickly has allowed the bad actors to plant seemingly realistic and plausible stories that are not properly vetted by these organizations and are propagated to viewers with the legitimacy provided by the news source.

In addition to the false stories placed in traditional media sources, actors have created their own news sources which create stories specific to their agenda which appear to come from a legitimate news source. The access to cable networks while costly has made this model very effective and can reach broad audiences.

Websites

Use of websites for organizations and disinformation topics provides the appearance of legitimacy, while some of these organizations may or may not actually exist. The actors use these sites to build followers and attract similar minded followers. The websites are protected by first amendment rights and provide a platform for the actors to craft stories that create false facts and stories.

Email

Emails are used to attract followers or entice targets to engage in the disinformation campaign by spreading false information and increasing fear. These emails are an easy and cheap way for cyber criminals to reach large groups and can be used to follow up on messages from other tools such as promoting a website, linking to social media or reinforcing stories from the traditional media sources.

MITIGATIONS

Protecting organizations and citizens from these attacks on our democracy require a multi-pronged approach. It has to involve all parts of society to reduce the effectiveness of these campaigns.

Government organizations, intelligence agencies and law enforcement organizations must collaborate and information share to identity the campaigns. They must inform the public of the existence of the campaigns and conduct take-down actions when appropriate to minimize the influence of foreign governments on the United States.

News organizations and social media platforms must make efforts to validate news sources and identify, eliminate or label false news so that their viewers are aware of the existence of the disinformation. They should also ensure that they clearly identify to their users which stories are opinion and which are fact-based reporting.

Businesses and social organizations need to stay engaged with both the media and their employees or members and ensure that there is an opportunity for social discussion but when necessary be prepared to engage in helping their communities understand how to access trusted information.

Citizens need to recognize that there are forces that benefit from divisiveness in society. When consuming news they must validate the source and where possible correlate the information with other sources before they make decisions and propagate the information to others.