White Paper

Leveraging Technical Expertise & Data Partnerships to Combat Disinformation

Argument - fierce, bold, and impassioned - has been at the heart of our American democracy since the founding.

British censorship (colonists could speak without prior restraint but then be charged with sedition or libel) compelled the drafters of the Bill of Rights to include freedom of speech as part of the First Amendment to the US Constitution.

Heated disagreement and even misinformation are as rampant on today's internet as they were in the taverns and meeting halls of the colonies.

This speech is rightly protected. But because of the sacredness of this right, it is disinformation – deliberate attempts by foreign and domestic actors to spread falsehoods in order to achieve a political end – that concerns us here at Nisos and that we leverage our capabilities to fight.

The goal of foreign meddling via disinformation is permanent unrest and debilitating internal conflict – "a house divided against itself cannot stand" -- and this tactic is as old as interstate conflict itself.

Powers through the ages have known that, as Sun Tzu wrote, "The supreme art of war is to subdue the enemy without fighting." The Romans perfected "divide and conquer" and Tacitus wrote of the Germanic tribes that "fortune can bestow on us no better gift than discord among our foes."

In a famous 2013 speech, Russian general Valery Gerasimov noted that "the role of non-military means of achieving political and strategic goals has grown, and, in many cases, exceeded the power of force of weapons in their effectiveness."

Foreign actors are deploying these age-old tactics against the United States with alarming regularity. Modern disinformation actors are sychologically astute. They latch on to legitimate grievances within a target population and amplify both sides of an argument to incite more violent reactions than would occur without the external intervention. Uncovering and rooting out such malign actors is an extraordinarily difficult task.

Disinformation: Four Parts

Nisos divides the problem of disinformation into four interlocking and cascading parts: narrative, outlet, account, signature.

Tracking narrative means identifying “what is being said” at both a strategic and tactical level by disinformation actors. There are numerous well-funded organizations that do excellent work tracking such narratives. While we ensure that our analysts and researchers have the domain expertise to distinguish between their Dugin and their Deng Xiaoping, narrative identification and tracking is not Nisos’ primary focus. Instead, Nisos leverages trusted partners’ narrative research in our efforts to use manual and technology-enabled means to identify and track the outlets that are pushing such narratives.

Beyond the well-known state-sponsored actors like RT, Sputnik, and CGTN, there is a thicket of tiny outlets whose content makes it into Western social media discourse on a regular basis. A large part of Nisos’ work is identifying these outlets and using advanced forensics and technology to uncover their ties to foreign actors.

Nisos also works to uncover the accounts that spread the narratives identified above or that are linked to the identified outlets. Like insurgents who blend in with the civilian population, individual disinformation actors’ accounts are often indistinguishable from legitimate domestic voices. Rare are the cases of easy tells like poorly spelled English and mangled syntax.

But even the most sophisticated actors make mistakes, and Nisos analysts’ decades of experience systematically tracking adversaries across cyberspace regularly enables us to uncover disinformation actors and then attribute their social media handles to their true identities.

Once we have identified outlets and actors, Nisos’s primary comparative advantage lies in our ability to map out the technical signatures of the identified outlets and accounts. We leverage multiple datasets plus technical forensics plus data analysis techniques, all cross-referenced with Nisos’s proprietary intelligence database.

This results in sophisticated understanding of the technical signatures of malign actors, which enables clients and partners to better monitor, blacklist, and track them even if they change superficial signatures such as social media handles.

The task of discovering, attributing, and tracking foreign influence has never been more daunting or more important. Nisos is always looking for partners to assist in this fight. Below is a list of some of the datasets we currently leverage in our disinformation practice. But we always need more.

If your company has access to such data and wants to partner with us on this urgent mission, we encourage you to contact us here.

- Relevant sources of legally available non-public datasets.
- Phone and email correlations to enable user attributions.
- Public data brokers.
- Social media bulk datasets.
- Financial databases.
- Foreign media sites, social media platforms, and legally available government databases.
- Mobile signals data.
- Global netflow data.
- Geolocation data, corporation associated IP’s, ad-tech data graph databases.
- DNS/WHOIS and threat intelligence content including indicator of compromise (IOC) artifacts—external threats, attackers, and their related infrastructure.
- Datasets containing internet facing devices (webcams, routers, servers, etc.).
- Credential pairs collected from public releases of breached datasets.
- Deep and dark web content.

Nisos is helping solve complex disinformation problems affecting some of the world’s most sophisticated platforms. But disinformation is a threat to businesses beyond major technology firms, since a coordinated disinformation campaign can significantly threaten company reputation and financial performance. We continue to evolve our capabilities and tactics, technology, and processes to stay abreast of this threat, both via internal innovation and trusted partnerships. Watch this space for updates on our journey.

During this remote-based activity period, previously implemented perimeter protection is irrelevant when the traffic flow does not pass through corporate network assets (i.e. proxy, firewall, NSM) for both Detection and Response. The lack of logging opens up new gaps of untraceable actions, for example accessing “threat sites” to include pastebins or competitor job sites, performing high volume/size uploads, or using log clearing software. For organizations which have not implemented public facing solutions for user behavior monitoring or endpoint management and security, these gaps force analytics of user pattern of life or behavioral review to be derived from severely limited datasets, often resulting in incomplete or inaccurate conclusions. Taking the time to lay down the appropriate security stack on your endpoints now is a giant step in the right direction and will set up your insider threat team for success when the users and assets come back to the office after we have weathered this storm.

For additional information, visit www.nisos.com or contact info@nisos.com.