The Art of Deception and the Role of Information Security Specialists

Kumar Setty and Arvin Verma

The dissemination of false information to achieve a desired result or reward is a technique as old as humanity itself. Throughout history, monarchs, governments, enterprises, armies and even individuals have engaged in this type of behavior to achieve a desired result. Disinformation is one of the critical elements in deception and in its applications in business, in warfare, in politics, and even during the intervals of peace. Since information integrity is critical in establishing trust in our institutions, information security professionals have an important role to play in countering deception and various types of disinformation as it will continue to be utilized not only by our adversaries but also ourselves and our allies to promote our interests.

Sun Tzu wrote in the fifth century in *The Art of War,*

> *All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.*[1]

Understanding the purpose and types of disinformation being utilized will help organizations and individuals better understand information being received as well as if the intention is to convey factual information or if its purpose is to drive other actions, whether it is for positive or negative results.

Understanding Misinformation

The art of using misinformation has been effectivity utilized by many countries for several thousand years but the Soviet Union and now Russia has been extremely effective with these types of activities. Starting in the 1920s, the Soviet Union engaged in active measures (*aktivnyye meropriyatiya*) or clandestine operations that were employed to further their political objectives. These active measures included misinformation and disinformation (*dezinformatsiya*) campaigns to discredit the United States and its allies. These types of measures were also effectively employed during the 1960s by the Soviet Union's KGB. Some examples include: [2]

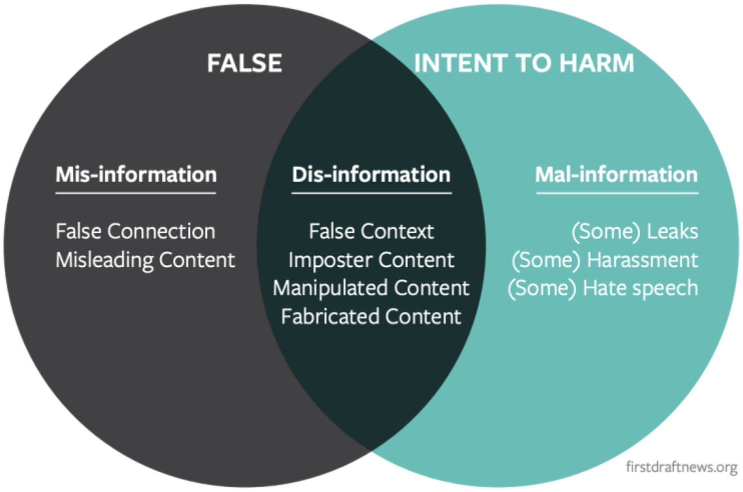
- According to the Center for Strategic and International Studies (CSIS), in 1968, the USSR secretly offered financial aid to US presidential candidate Richard Nixon's opponent, Hubert Humphrey, who flatly refused this aid. In addition, the USSR also actively campaigned against Ronald Reagan's presidential campaign.
- Soviet intelligence services fostered and disseminated a disinformation campaign through various media outlets stating that the origin of the acquired immunodeficiency syndrome (AIDS) virus was from a US military lab. This story was then disseminated and printed in newspapers and reported in news outlets throughout Africa. The stories were printed as a result of bribes to newspaper editors.[3]
- In 2013, a fake press release was accidentally promoted by many trusted news outlets, damaging one enterprise's reputation and bottom line. The false release indicated that The Australia and New Zealand Banking Group Limited (ANZ) was withdrawing $NZ 1.2 billion in funds from Whitehaven Coal. A wire journalist rushed to release the story before confirming the source. The person responsible for the forged press release was an anti-coal activist. However, spooked investors dumped Whitehaven stock and shaved off $NZ 300 million from the market capitalization of the company before the damage was undone.[4]

- Most recently, after the 2016 US presidential campaign, a series of exposes revealed the machinations of Cambridge Analytica. This firm had logged Facebook data in a database used by political campaigns. The information of 50 million Facebook users had been inadvertently collected and used to target segments of supporters.[5]
- [In the current situation involving Russia and Ukraine, the Russian government ironically asked Google to block YouTube content detailing activities of the Ukrainian information, claiming it was misinformation and propaganda. [6]]

The most widespread examples include "fake news" or "fake media." Unfortunately, these phrases are highly politicized and used by people to disparage news outlets or stories with which they might not agree, despite their veracity. Fact checking and censor checking is outside the scope of this article.

Much of the discourse on fake news conflates two notions: misinformation and disinformation. But there is a clear distinction between the two terms, as well as a third term: "malinformation."

Figure 1



Source: United Nations Educational, Scientific and Cultural Organization (UNESCO), *Journalism, Fake News and Disinformation,* UNESCO Series on Journalism Education, France, 2018, *https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf*

Misinformation

Misinformation is information that is false, but the person who is disseminating it believes that it is true. For instance, an individual might post a false fact on Facebook, but they may believe that the post is true, and others may agree with the posting.

Disinformation

Disinformation is information that is false, and the person who is disseminating it knows it is false. It is a deliberate, intentional lie, and it is used by malicious actors to actively disinformed people. Examples of disinformation include the aforementioned examples of the Soviet intelligence services. One particularly harmful example is deepfakes. Deepfakes (a portmanteau of "deep learning" and "fake") use deep learning artificial intelligence to replace the likeness of one person with another in video and other digital media. So, one could create a likeness of a US President or another prominent person and superimpose this likeness on another person speaking on another topic or expressing completely different or controversial views.

Another example is a fake Twitter or Facebook account that is used to propagate falsehoods. As shown in **figure 1**, disinformation is distinct in that it straddles both categories of false and intent to harm.

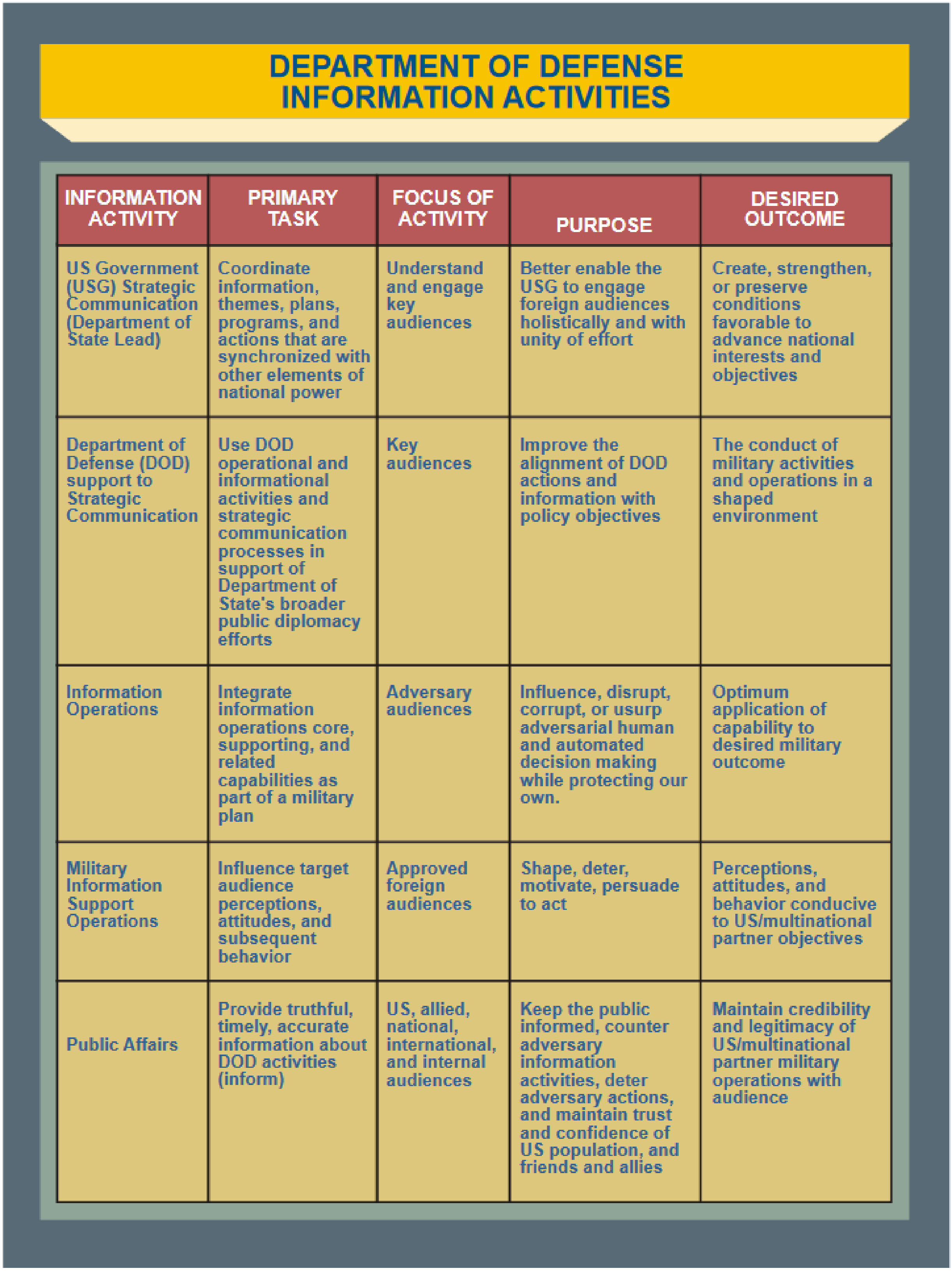
Malinformation

Malinformation is information that is based on reality, but used to inflict harm on a person, organization or country. An example of this is a report that reveals sensitive personal information without the justification of public interest. It is important to distinguish messages that are true from those that are false and those that are true but have been created, produced, or distributed by agents who intend to harm rather than serve the public interest. Such malinformation goes against the standards and ethics of journalism.[7]

Another example of malinformation could be a leak from an organization that is about to lay off many employees.

US Military Operations with Disinformation

The United States military has utilized disinformation with its various efforts in war as well as peace but within the bounds of the US/UN laws and ultimately the US Constitution. A break down these different types of activities:



DEPARTMENT OF DEFENSE INFORMATION ACTIVITIES

INFORMATION ACTIVITY	PRIMARY TASK	FOCUS OF ACTIVITY	PURPOSE	DESIRED OUTCOME
US Government (USG) Strategic Communication (Department of State Lead)	Coordinate information, themes, plans, programs, and actions that are synchronized with other elements of national power	Understand and engage key audiences	Better enable the USG to engage foreign audiences holistically and with unity of effort	Create, strengthen, or preserve conditions favorable to advance national interests and objectives
Department of Defense (DOD) support to Strategic Communication	Use DOD operational and informational activities and strategic communication processes in support of Department of State's broader public diplomacy efforts	Key audiences	Improve the alignment of DOD actions and information with policy objectives	The conduct of military activities and operations in a shaped environment
Information Operations	Integrate information operations core, supporting, and related capabilities as part of a military plan	Adversary audiences	Influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.	Optimum application of capability to desired military outcome
Military Information Support Operations	Influence target audience perceptions, attitudes, and subsequent behavior	Approved foreign audiences	Shape, deter, motivate, persuade to act	Perceptions, attitudes, and behavior conducive to US/multinational partner objectives
Public Affairs	Provide truthful, timely, accurate information about DOD activities (inform)	US, allied, national, international, and internal audiences	Keep the public informed, counter adversary information activities, deter adversary actions, and maintain trust and confidence of US population, and friends and allies	Maintain credibility and legitimacy of US/multinational partner military operations with audience

Figure II-1. Department of Defense Information Activities

The three key areas which fall under the scope of this article are MILDEC – Military Deception, MISO – Military Information Support Operations and PA – Public Affairs.

- MILDEC focuses on using false information to promote efforts, think of this as fake news.
- MISO is using factual information to sway opinions in the positive direction
- Public Affairs is solely focused on presenting the facts, regardless of the message being positive or negative.

While these methodologies were developed and currently utilized for military use of force, they are now entering the civilian side. Combating these efforts will require significant efforts by both our technical and non-technical stakeholders but we recommend starting with the most obvious first line of defense – Cybersecurity/IT Audit

The Role of IT Audit/Modern Day Cybersecurity

The prevention and remediation of disinformation and malinformation should weigh heavily within the job responsibilities of IT auditors. Prevention and responses to misinformation campaigns historically have not been within the scope of IT auditors but to remediate this situation, we recommend asking more from audit teams. In addition, partnership with corporate affairs, marketing, and public affairs, malinformation in the form of leaks may be treated as data breaches but the impact to the customer, brand reputation and other factors need to be taken into consideration and by having this level of partnership, then we can only begin defending against these nefarious activities. Prevention and remediation of data breaches is very much within the duties of most IT auditors and information security professionals. Often times, cybersecurity professionals forget our base foundation, the CIA Triad. Despite it appearing that disinformation/malinformation efforts focuses on only the integrity part or the confidentiality part, they are not limited to these areas. Resolving an effort like this requires all three domains of the CIA triad and the various cybersecurity domains such as those listed below to help drive preventive and detective capabilities to address malinformation. The following are just a starting point:

- Endpoint security
- Data loss prevention (DLP)
- Management of identities and privileges
- Data security
- Network security
- Authoritative Sources

It is difficult to predict when or from where a disinformation campaign may originate, but once it is detected, an organization can take certain steps to ameliorate this type of negative campaign. Organizations should be proactive in the following ways:

- Organizations should publicize a statement or policy that reinforces their commitment to rooting out any internal sources of disinformation such as disgruntled employees and other possible false sources of information from other countries or competitors. There should be an internal media relations department that curates and approves any news or events.
- Organizations should provide the public a way to report any disinformation such as false financial news or other disinformation or misinformation.
- Organizations should create a reporting structure and procedures for addressing disinformation. There should be specific metrics such as time to resolution. This can be similar to disaster recovery exercises.

- IT auditors in cooperation with IT security should periodically assess their organization's vulnerabilities with respect to disinformation This should be approached like any other vulnerability assessment.

Figure 2—**An Elementary Control Framework for Assessing Vulnerabilities to Disinformation**

RISK	**CONTROL**	**TEST METHOD**
The public does not understand an organization's stance on fake news or false information.	The organization clearly outlines its stance to the public on the topic of disinformation, malinformation and misinformation.	1. Verify that a policy addressing disinformation, malinformation and misinformation exists on the website. 2. The policy should clearly outline that the organization understands the risk; provides examples; and discloses any previous disinformation campaigns, penalties, actions and legal remedies the organization will pursue in response to a negative information campaign.
The public or media outlets have no way of reporting false news stories or negative campaigns against the organization.	The organization has outlined and publicized procedures and contact information for reporting negative information campaigns.	1. Test the reporting procedures and contact information to ensure that the content is accurate and current.
The organization does not monitor social media or news outlets, so it is not	The organization monitors all social media outlets and news outlets and is immediately alerted regarding any negative information campaigns.	1. Test all monitoring methods and systems. 2. Test and measure the response times and

aware of any negative information campaigns.		remediation times in response to any negative information campaigns.
The organization does not respond to any negative posts on social media.	The organization actively monitors negative posts and immediately responds to any negative posts.	1. Verify the procedures for responding to negative posts.

Conclusion

The issue of employing deception to achieve a political, economic, or commercial goal will only accelerate in the coming years. Utilizing partnership efforts between private/public companies and governmental agencies such as the ISAC's, FBI's InfraGard and DHS's HSIN is one additional way that these disinformation campaigns can be caught/identified and effectively responded to, including obtaining federal government and military resources. These efforts by bad actors are no longer small efforts with little to no resulting action, but to an extent terroristic actions and as a result should be catalogued and communicated to government agencies to help drive stronger legislation and responses as these incidents increase.

IT audit and security professionals should understand this threat and treat it as any other attack vector. We recommend that organizations assess the risks and adverse outcomes of being exposed to information deception attacks.

Kumar Setty *is the Principal of Zakti Security Labs. He has over 20 years of experience in cybersecurity and fraud risk assessment. Mr. Setty has assisted many private and public companies, and government agencies in protecting their information. He has also assisted in remediating some of the largest data breaches ever recorded. Mr. Setty has a Master of Science in Software Engineering from Carnegie Mellon University, an MBA from the University of Illinois, and a Bachelor of Science in Chemical Engineering from the University of Rochester. He is a member of InfraGard Chicago and holds the following certifications: CISSP, HCISPP, CISA, QSA, PCIP, CCSK, and ITIL. Mr. Setty is also a member of Mensa and InterTel, and author of the upcoming book, "The CISO Workbook – A Guide for Securing Your Startup".*

Arvin Verma *is a highly motivated cybersecurity professional, with over 10 years of experience across a multitude of cyber and IT domains. He has worked in multiple industries spanning over 5 Fortune 500 companies and Big 4 consulting. In addition, Arvin is proudly serving as a direct commission officer in the US Navy Reserves as a Cryptologic Warfare Officer. serves as a research fellow with the Cybersecurity Forum Initiative where he has co-authored several research papers in new cyber trends and best practices and holds several leadership positions with InfraGard Chicago and InfraGard National. He also serves as an advisor to several private and public entities and is a guest lecturer at several universities across the State of Illinois. Arvin is ISC2 CISSP certified, CompTIA Security+ certified and ISO 27001 Lead Auditor certified.*

Endnotes

[1] Tsu, S.; *The Art of War*,

[2] Payton, T.; *Manipulated: Inside the Cyberwar to Hijack Elections and Distort the Truth*, Rowman and Littlefield, USA, 2020

[3] Ibid

[4] Ibid

[5] Ibid

[6] https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-03/card/russia-demands-google-block-false-ads-about-ukraine-war-RxxXhZMePtDOZ9mRu15U

[7] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Journalism, Fake News and Disinformation,* UNESCO Series on Journalism Education, France, 2018, *https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf*