NIGHTDRAGON

MARKET REPORT:

DISINFORMATION

June 2024

www.nightdragon.com

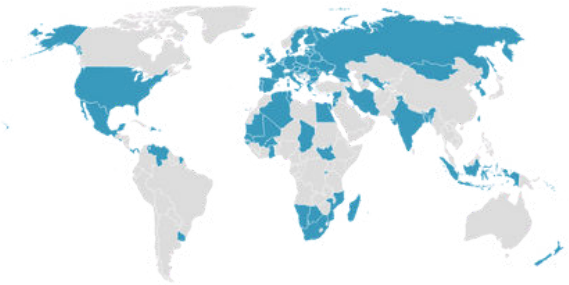
Foreword

Every time we navigate the Internet or our daily lives we are faced with an important question: what is true, and what is not?

This is the challenge we face today given the rise of disinformation.

Disinformation is false information deliberately, and often covertly, spread to influence public opinion or obscure the truth. While this false information is often spread over social media, it also inevitably finds a home on numerous other digital channels. (Note that the intent makes this different from misinformation, which is incorrect or misleading information but not necessarily with malicious intent).

Disinformation was named one of the top global risks by the World Economic Forum in 2024, with the group's Global Risks Report citing that the "nexus between falsified information and societal unrest will take center stage amid elections in several major economies that are set to take place in the next two years." These threats are growing at a significant pace - and don't seem to be slowing down.



Countries holding elections in 2024

We're already seeing the negative effects of these disinformation campaigns in action. Disinformation across social media and other communications channels has caused chaos to erupt in Ecuador, Ukraine, the United States, and other countries around the world in the last few years. This year, we expect over half the world's population to head to the polls across 80 countries, and disinformation campaigns pose significant concerns. What's more, businesses are seeing their brands impacted through the spread of negative information or experiencing fraud to the tune of millions of dollars as the result of deepfakes or other malicious tactics.

As is the case whenever there is a significant dislocation between offense and defense, we see a significant market opportunity arise for innovators able to mitigate risk using artificial intelligence or other technologies. As one sign of this growth, we saw $248 million invested in 2023 and $79.9 to date in 2024 (on track to meet or exceed 2023 numbers), according to Altitude Cyber, and many interesting startups emerging and gaining traction in the market.

In this report, we'll explore the threat landscape as it pertains to disinformation, as well as the new technology categories emerging in this sector. We have also spoken to many experts from the NightDragon Advisor Council, who share insights into what technologies are being put into action today, how they're evaluating innovation, as well as the latest research and trends.

NightDragon continues to evaluate new markets as they arise to ensure we are abreast of the latest technologies and trends to make informed investment decisions. We will continue to release market reports on those sectors we believe hold interest or promise to be meaningful market segments or present significant opportunity.

Table of Contents

The Challenge

The concept of disinformation isn't new. One of the first recorded uses of the term tracks to the 1890s, though its prevalence and impact has heightened significantly in our digital world. Attackers are becoming increasingly sophisticated, with select nation-states elevating it to a key part of their digital strategies and attackers launching shadow industries similar to what we have seen play out with malware, where techniques are sold both as a product and as a service.

A combination of AI and excessive time spent online (an average of 7 hours and 43 minutes a day in the US) has created a prime breeding ground for highly targeted (and realistic!) content creation in the form of text, photos, and videos. Thus, creating awareness around disinformation and its prevalence across all forms of media has never been more important, as 56% of internet users (in 16 countries) cite social media as their primary source of news.

Growing Threats

70% False information is 70% more likely to be reshared than truth

23% Only 23% of adults in the US feel confident in their ability to recognize false information

900% The market for deepfakes grew 900% between 2019 and 2020

90%

90% of online content is predicted to be synthetically generated by 2026

66%

66% of CISOs and cybersecurity professionals reported experiencing deepfake attacks in 2022

Types of Threats

NATION STATES	NON-STATE ACTORS
Nations such as Russia, Iran, China and North Korea are actively using disinformation campaigns as part of their foreign policy doctrines. Example: China sowed disinformation about the fires in Maui in 2023, calling the disaster not natural, and a "weather weapon" of the United States. The campaign leveraged AI and represented a growth in Chinese tactics around disinformation, said researchers.	Domestic and cyber criminals leveraging disinformation or deepfakes to execute phishing, fraud, ransomware and other types of attacks. Example: A finance employee in the UK paid $25 million for a "secret transaction" after a deepfake video conference call with someone he thought was the CFO.

"Both of these categories are continuing to grow. These issues are so pervasive that the education and defense around them will need to be too. We must invest in companies that are providing strong and innovative solutions."

– Dr. Bilyana Lilly
Author of "Russian Information Warfare"

As disinformation continues to rise as a risk category, its impacts can be significant. Some notable areas of potential harm for both enterprises and individuals include:

SOCIETAL DISRUPTION

The spread of disinformation online has sown distrust in political systems and processes and contributed to increased polarization and chaos. This sentiment has, unfortunately, led to erratic and devastating consequences. For example, an 18-year-old in Buffalo, New York committed a mass shooting, citing false online narratives as the driver for his actions. As a result, ten individuals were killed, and three were injured.

FINANCIAL

Publicly traded companies in the US lose about $39 billion annually due to disinformation-related stock market losses, while $78 billion globally is lost each year. For example, in May 2023 a deepfake of an explosion in the Pentagon spread on X (formerly Twitter). Minutes later, the stock market plummeted by half a trillion dollars.

REPUTATIONAL DAMAGE

Disinformation can spread negative rumors or false information that can harm a business or individual's reputation. Organizations with as few as four negative articles can experience losses of up to 70% of prospective customers.

OPERATIONAL DISRUPTION

Disinformation campaigns surrounding an organization's products, services, or operations can lead to disruptions to supply chains and partnerships. For example, disinformation around COVID-19 led to conspiracy theories that 5G caused the illness. This led to arson attacks against telecom infrastructure in the UK and other areas.

CYBERSECURITY

Disinformation through phishing and CEO fraud are other risk areas, where a highly trained deepfake is used to impersonate an organization's top leaders. For example, a British energy provider CEO transferred €220,000 to a scammer who had digitally mimicked the head of his parent company.

LEGAL AND REGULATORY

Disinformation campaigns can also violate laws and regulations related to defamation, intellectual property rights, consumer protection, and data privacy. For example, in 2018, the Securities and Exchange Commission (SEC) charged numerous hedge funds for shorting firms and spreading disinformation about them.

Market Opportunity

We are seeing new innovators emerge around these solution vectors, garnering venture capital investment and even M&A interest. While many of these companies are earlier stage, the total addressable market potential for this sector appears to be significant as the risk grows. Below, you can find an overview of funding growth in the sector.

"The market is only going to get bigger…you can access anyone in the world in a second, so this issue will persist."

- Heather McMahon
Founder and CEO, Artemist Advisory

Venture Investment

Financing Summary	2022	2023	2024 (YTD)
Aggregate Financing Value ($M)	$233.4	$248.0	$79.9
Number of Deals	24	31	7
Average Deal Value ($M)	$12.3	$9.9	$11.4

Source: Altitude Cyber
*Note 2024 values represent through April 2024 only

Financing by Size

Financings By Funding Type	2022		2023		2024 (YTD)	
	Activity	Total Volume ($M)	Activity	Total Volume ($M)	Activity	Total Volume ($M)
Debt	2	$110.0	0	$0.0	0	$0.0
Other	0	$0.0	0	$0.0	0	$0.0
Early Stage	15	$11.4	17	$28.1	3	$29.0
Series A	3	$40.0	5	$73.9	2	$24.0
Series B	1	$32.0	3	$25.0	1	$20.0
Series C+	3	$40.0	6	$121.0	1	$6.9
Total	24	$233.4	31	$248.0	7	$79.9

Source: Altitude Cyber

*Note 2024 values represent through April 2024 only

Market Categories

Various organizations are pushing efforts to mitigate the creation and spread of disinformation by finding, analyzing, and correcting false information. Others work to protect brand reputation through the detection of harmful or untrue narratives, attacks led by bots, or utilization of deepfakes. Though AI is perhaps more commonly thought of as the enemy, many companies are using the same tool to defend true claims.

See below for a selection of how companies are creating technology to fight disinformation:

CONTENT REVIEW

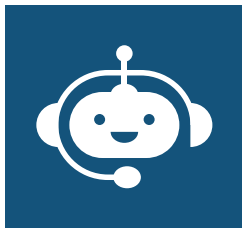
Human-based or machine learning technologies to help identify written disinformation online. Some platforms leverage a scoring technique to review and score content for authenticity, while others protect against hate speech and harmful content.

DISINFORMATION COUNTERMEASURE

Identify potentially harmful disinformation and work to de-escalate disinformation before false narratives can spread

ONLINE BRAND ABUSE

Detect and alert organizations of disinformation spreading about its brand specifically on social platforms



BOT DETECTION

Providing services to safeguard organizations from online bots that can be responsible for fraud and account abuse

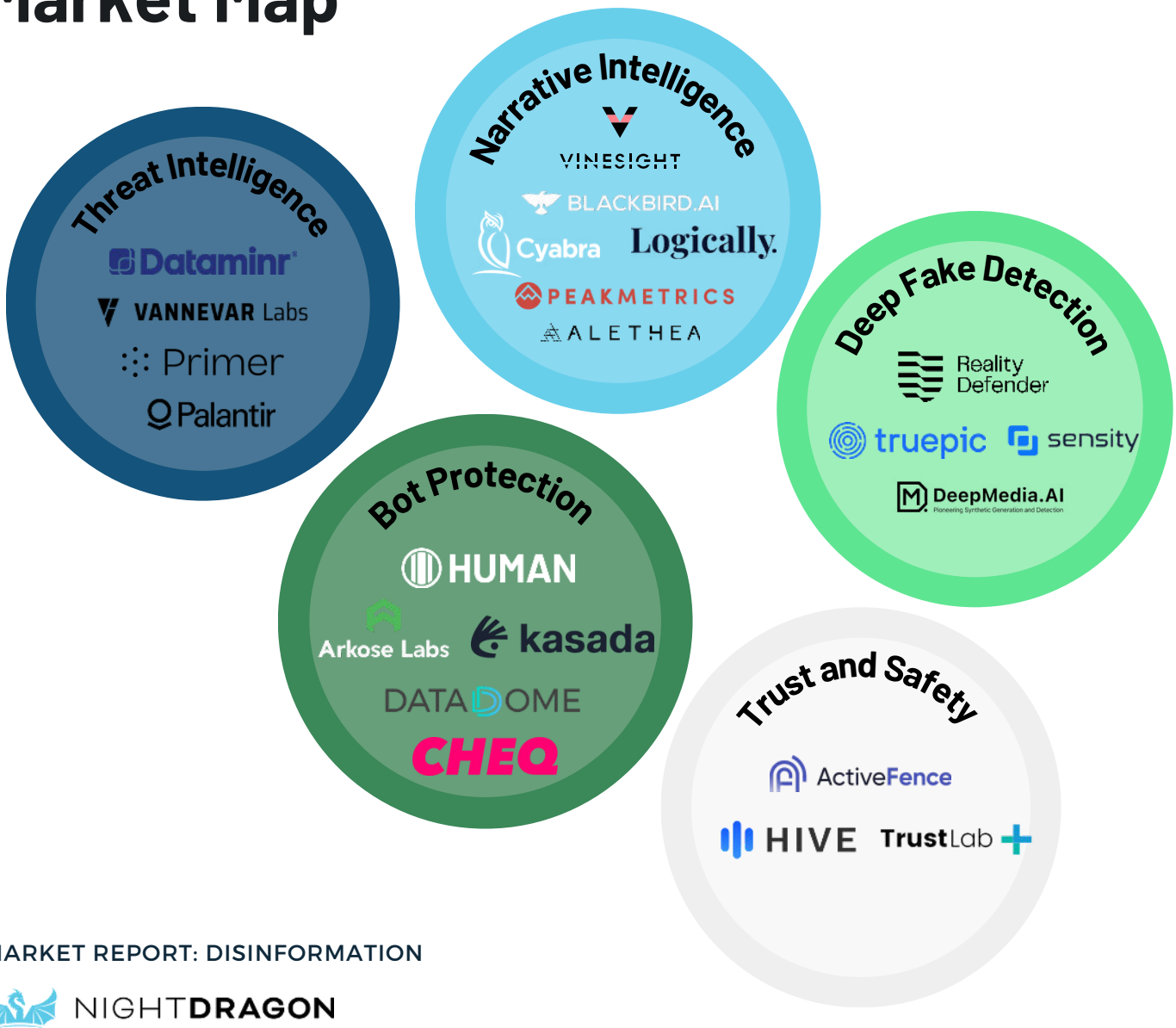
DEEPFAKE DETECTION

Leveraging technology solutions and machine learning to identify potential forgery, false imagery or videos, or deepfakes

USER VERIFICATION

Leveraging technology such as biometrics to validate a users' identity to differentiate it from false or digitally created content

Market Map



Understanding the Buyer

Combating disinformation will most likely be accomplished through a multifaceted effort from the public and private sectors, as well as nonprofits and the individuals interacting online every day. Each of the buyers listed below plays an important role in fighting disinformation:

More Established Buyers:

- Governments – Governments are the primary purchasers of misinformation and disinformation technology today, largely due to critical implications around national security. From its potential to disrupt elections to distorting public perception of significant global events, the threat of disinformation is a paramount concern for governments worldwide.
- Platform Companies – Platform vendors such as telecommunications or social media companies are buyers of disinformation technology to incorporate into their platforms and prevent disinformation from spreading at its source. These purchases are also spurred by government regulation.
- Chief Marketing Officers – CMOs are interested buyers as they look to monitor and protect the company brand and reputation online.
- Trust and Safety – Trust and safety leaders, the exact title of which may vary by organization, are also buyers of disinformation technology with brand and compliance focuses in mind.

Emerging Buyer Personas:

- Chief Information Security Officers - While many CISOs are more focused on short-term cyber threats, some are interested in mitigating disinformation risk. This appears to be mostly on a case-by-case or "as-needed" basis.
- Chief Compliance Officers – CCOs prioritize preventing and monitoring malicious content and disinformation to uphold regulatory, compliance, and ethical standards within organizations. Investing in content moderation or misinformation prevention tools enables CCOs to address these challenges proactively.
- Chief Legal Officers - CLOs prioritize preventing disinformation, deepfakes, and malicious content due to the legal risks they pose. In today's digital world, these issues can lead to defamation lawsuits, IP infringement claims, and regulatory fines. Deepfakes also raise concerns about identity theft and fraud.

NightDragon Perspective

As a SecureTech (investing in cybersecurity, national security, and adjacent sectors) firm, we evaluate market opportunities by assessing the gap between offense and defense. In the disinformation market, there has historically been a significant gap between the offensive tactics used by bad actors and the defensive measures available to protect against them. This gap is only widening due to the proliferation of social media, other digital channels, and the rapid advancement of AI technologies.

Currently, the market is still in its early stages, with buyer personas and use cases still evolving. While government agencies, CMOs, and Trust & Safety organizations are established buyers, we believe this market will increasingly become relevant to cyber organizations as misinformation and disinformation evolve into critical threat intelligence signals. Companies capable of breaking down organizational silos and building comprehensive platforms to address the multifaceted challenges the market presents have the potential to grow into market leaders. There is also the opportunity for companies, especially those leveraging AI, to advance monitoring to include predictive capabilities, which can enhance our risk visibility today but also model what might happen tomorrow for better risk mitigation.

Contact Us

If you're building interesting technology in this sector or have a perspective on disinformation, please reach out to the members on our team following this market:

Morgan Kyauk
Managing Director
morgan@nightdragon.com

Hannah Huffman
Vice President
hannah@nightdragon.com

NIGHTDRAGON