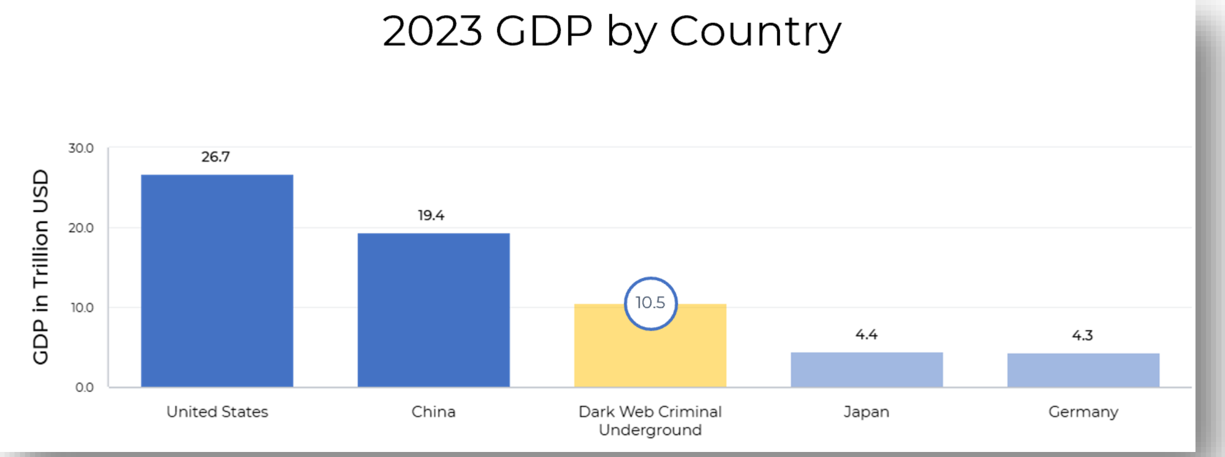
# The Case for Cyber Threat Intelligence to Combat Election Threats

### AI, the Cybercrime Gig Economy, Nation States, and MDM

## Introduction

Election integrity threats have evolved significantly over the past several years, becoming increasingly sophisticated and diverse in nature. As digital technologies have advanced, so too have the methods employed by malicious actors aiming to undermine electoral integrity. Election interference is no longer limited to traditional forms of manipulation; it now encompasses a range of tactics, including cyberattacks, disinformation campaigns, and social media manipulation.

The criminal underground, sometimes referred to as the "darkweb market" has monetized election interference. Cybercrime has become so lucrative that it's now a part of the "gig economy." If the cyber-criminal underground was a country, it would have the third largest GDP behind the US and China.

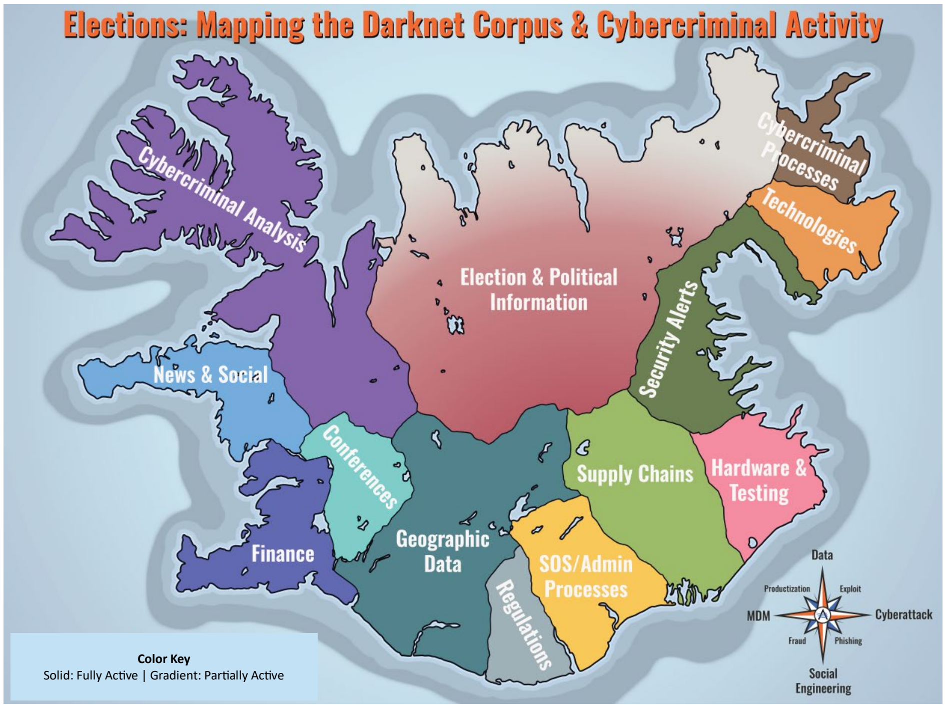


This evolution has heightened the importance of cybersecurity in safeguarding elections, as even minor breaches can lead to substantial disruptions and loss of public trust in democratic processes.

Cybersecurity plays a crucial role in protecting election systems from myriad threats. It involves implementing advanced measures to secure sensitive information, systems, and operations against unauthorized access and malicious activities. Threat intelligence analysts are essential in this fight, as they gather and analyze data about potential threats, helping election officials to anticipate and mitigate risks. Their expertise allows for real-time monitoring of cyber threats, enabling proactive responses to emerging vulnerabilities.

### Key actors involved in election interference:

- **Nation-States**
  - Motivated by geopolitical goals, Nation-states engage in sophisticated cyber operations to influence public opinion and disrupt electoral processes in rival countries. For instance, known actors like Russia and China have been implicated in orchestrating large-scale disinformation campaigns aimed at swaying voter sentiment.
- **Cybercriminal Groups – The "Gig Economy"**
  - typically seek financial gain through tactics such as ransomware and phishing. These groups may exploit election cycles to launch targeted attacks against election infrastructure.
  - Criminal groups have created a network of services similar to the app store on your device.
- **Individual Malefactors – "Dark Investors" and "Dark Lobbyists"**
  - Cryptocurrency funded PACs and even lobbyists
  - Contribute to the spread of misinformation, often through social media platforms, further complicating the election security landscape.



Overall, the increasing complexity of election interference threats necessitates a robust response from election officials, cybersecurity experts, and the public to maintain the integrity of democratic processes and ensure that elections remain free and fair.

Election interference through information manipulation has significantly threatened democratic processes worldwide. Understanding the distinctions between misinformation, i sãs| p~ä{ ^és~| Ø^| i malinformation is crucial for election officials and cybersecurity experts to combat these threats effectively.

## Misinformation, Disinformation, & Malinformation (MDM)

- **Misinformation** refers to false information that is spread without the intention of causing harm. In the context of elections, this might include voters sharing incorrect polling times or locations on social media, believing they are helping others. While not malicious in intent, misinformation can still lead to voter confusion and reduced turnout
- **Disinformation**, on the other hand, is deliberately created and spread with the intent to deceive. Cybercriminals and foreign actors often employ disinformation campaigns to manipulate public opinion and influence election outcomes. For example, Russia has been known to use this tactic on social media platforms to sow discord and undermine trust in democratic institutions
- **Malinformation** involves the sharing of genuine information with the intent to cause harm by manipulating its context. This tactic is particularly insidious as it leverages truth to mislead. For instance, cybercriminals might selectively edit videos of political candidates or exaggerate minor election irregularities to suggest widespread fraud

Cybercriminals employ various tactics to spread these forms of information:

1. **Social media manipulation**: Creating fake accounts and using bots to amplify false narratives
2. **Phishing campaigns:** Targeting election officials and staff to gain access to sensitive information.
3. **Hack-and-leak operations:** Stealing and selectively releasing information to influence public opinion
4. **AI-generated content:** Using artificial intelligence to create convincing deepfakes and synthetic media

A notable example of disinformation occurred during the 2016 U.S. presidential election when Russian operatives created fake social media accounts to spread divisive content and influence voter behavior

More recently, the use of AI-generated content has raised concerns about the potential for highly convincing deepfakes to mislead voters

To combat these threats, election officials are implementing multi-faceted approaches:

1. Collaboration with social media platforms to quickly identify and remove false information
2. Public education initiatives to improve digital literacy and critical thinking skills
3. Implementation of advanced cybersecurity measures to protect election infrastructure
4. Rapid response teams to address emerging narratives and provide accurate information

As the landscape of election interference evolves, election officials, cybersecurity experts, and the public must remain vigilant and adaptable. By understanding the nuances of misinformation, disinformation, and malinformation, stakeholders can better protect the integrity of democratic processes and maintain public trust in elections.

## Current Cyber Threats to Elections

In today's digital landscape, elections face a multitude of cyber threats that can significantly undermine the integrity of the electoral process. Among the most pressing concerns are phishing attacks, ransomware targeting voter databases, Distributed Denial-of-Service (DDoS) attacks against election portals, and hack-and-leak operations. Each of these tactics poses unique challenges for election officials and cybersecurity experts alike.

- **Phishing attacks** remain one of the most prevalent cyber threats against election officials. These attacks typically involve misleading emails that appear legitimate, tricking recipients into divulging sensitive information, or inadvertently downloading malware. For instance, the "SocGholish malware campaign in 2024 specifically targeted election officials through tailored phishing emails, demonstrating the cunning nature of cybercriminals. Such attacks not only compromise individual accounts but can also lead to more significant breaches within election infrastructure.

- **Ransomware** is another critical threat, mainly targeting voter databases and election management systems. The 2024 incident involving Coffee County, Georgia, exemplifies this danger. In this case, a ransomware attack forced the county to disconnect from its voter registration system, raising alarms about the potential for widespread disruption during election periods. Ransomware can paralyze critical systems, making it nearly impossible for election officials to access necessary data or conduct operations seamlessly.

- **DDoS attacks** pose a further risk by overwhelming election websites with traffic, rendering them inaccessible. These attacks can disrupt voter information dissemination and compromise the reporting of election results, eroding public confidence. Cybercriminals often employ DDoS attacks during key election periods to maximize their impact, targeting state and local election websites to create chaos.

- **Hack-and-leak operations** represent a more insidious form of interference. In these operations, unauthorized access to sensitive information is followed by the selective release of data to manipulate public perception. This tactic was notably used against political campaigns in past elections, where stolen information was strategically leaked to sway voter opinions.

Collectively, these cyber threats underscore the urgent need for robust cybersecurity measures and proactive strategies to safeguard electoral processes. By understanding and addressing these tactics, election officials can better protect the integrity of democratic systems and maintain public trust.

## Recommendations for Enhancing Election Security Measures

To strengthen the security of election infrastructure and ensure the integrity of democratic processes, a multi-faceted approach is essential. Drawing from best practices, for instance, those implemented by Maricopa County, several actionable recommendations can be outlined.

### Engage with a Cyber Threat Intelligence Firm

One of the most effective strategies for securing elections is to work with a CTI firm that specializes in "man in the room" tactics. It takes decades of experience and informant cultivation to access the groups that sell data, tools, and services that can impact elections.

### Conduct Tabletops, Rigorous Testing and Audits

Tabletops at the County and State level are fun, terrifying, and completely necessary for the future.

Rigorous testing and auditing of election infrastructure are vital to maintaining public confidence in electoral processes. States should conduct logic and accuracy testing of voting systems prior to elections, ensuring that all equipment functions as intended. Additionally, post-election audits can verify the accuracy of results by randomly selecting batches of ballots for hand counting.