The Weaponization of Emotion: Micro-Targeting ANCODI in Vulnerable US Communities for Destabilization and Radicalization

I. Executive Summary

This report examines the sophisticated strategies employed by both state-sponsored and criminal actors to identify and exploit demographic and socioeconomic vulnerabilities within US communities. The core mechanism of this exploitation is the precise cultivation and amplification of Anger, Contempt, and Disgust (ANCODI) emotions, which are foundational to hatred and intergroup aggression. This emotional manipulation is designed to foster localized destabilization and radicalization, posing a significant threat to national security and social cohesion.

Key findings reveal that digital tools, including social media, the dark web, and advanced artificial intelligence (AI), are critical enablers for micro-targeting, allowing actors to tailor emotionally charged narratives to specific vulnerable populations. Both state and criminal entities leverage pre-existing grievances, economic insecurity, and social isolation to erode trust in institutions and foster an "us vs. them" mentality. The resulting destabilization manifests as increased polarization, civic disengagement, and a heightened risk of violence, with profound consequences for public safety and democratic processes.

II. Introduction: Defining the Threat Landscape

A. The ANCODI Hypothesis: Emotional Foundations of Hatred and Aggression

The ANCODI (Anger, Contempt, and Disgust) hypothesis posits that these three emotions are the fundamental components of hatred and are strongly linked to intergroup aggression and hostility. Understanding the distinct functional roles of each emotion, and their combined effect, is crucial for comprehending how malign actors manipulate them to achieve destabilizing objectives.

Anger, from a functional perspective, facilitates the removal of obstacles. In the context of intergroup relations, anger can shift from a temporary assessment of a group's behavior to a more permanent one. When anger occurs separately from contempt and disgust, it more often motivates participation in normative social actions, such as protests, petitions, or civil disobedience. This indicates that initial anger, while potentially leading to legitimate forms of protest, can be a precursor to more extreme emotional states if manipulated.

Contempt makes a statement about inherent moral superiority. It is an emotion that is manufactured more slowly and is activated by the idea that common norms and values are being violated. Contempt is associated with non-normative social actions, such as sabotage, violence, or terrorism, and allows for the devaluation of the outgroup. The slow cultivation of contempt is particularly concerning as it implies a deliberate, sustained campaign to undermine the perceived worth and legitimacy of a targeted group.

Disgust helps to eliminate or repulse contaminated objects. This emotion is directly linked to violent actions against the outgroup, its devaluation, and ultimately its elimination. Disgust is associated with the process of dehumanization and is aroused by violations of moral norms of purity and sanctity. The progression to disgust signifies a critical and dangerous stage in emotional manipulation, as it psychologically primes individuals for extreme aggression.

The ANCODI hypothesis posits that when anger, contempt, and disgust are directed against an outgroup, these negative emotions collectively motivate hostility and violence towards that group. Hatred is described as a distinct yet composite feeling comprising elements of anger, contempt, and disgust, emerging when these three emotions are activated simultaneously in varying degrees. Compared to individual emotions, hatred is experienced as more emotionally arousing, targets are perceived as more threatening, and individuals are more willing to attack them. Research provides initial evidence for the causal role of ANCODI in producing hostile cognitions and competitive decision-making. Studies examining speeches by leaders of extreme political groups demonstrate elevated ANCODI emotions and precursor appraisals three months prior to violent events, highlighting their predictive power. The ANCODI hypothesis can be viewed as both a "sensor" of an individual's internal emotional state, indicating an active urge to fight against a perceived cause, and an "effector," meaning this emotion mix can be communicated to generate hatred in other individuals, thereby serving as a tool to analyze manipulative intentions.

The progression from anger to contempt and then to disgust represents an escalation ladder of emotion that can lead to violence. The functional outcomes of each ANCODI emotion are distinct: anger often leads to normative social actions, contempt to non-normative actions, and disgust to the desire for elimination and dehumanization. When these emotions are combined, they explicitly culminate in hatred and violence. This suggests a deliberate, progressive manipulation: initial anger at perceived wrongdoing can be systematically transformed into contempt, leading to devaluation, and then into disgust, fostering a desire for elimination. This pathway moves individuals from potentially peaceful protest to violent aggression, a critical process that malign actors exploit for radicalization. The cultivation of ANCODI, particularly disgust, serves as a deliberate psychological tactic to enable violence by stripping the target group of their humanity, thus overcoming moral sanctions against aggression. This is a crucial step in escalating from emotional manipulation to violent action.

Table 1: ANCODI Emotions and Their Functional Contributions to Intergroup Aggression

Emotion	Functional Perspective	Associated Actions
Anger	Facilitates removal of obstacles; shifts from temporary to permanent assessment of group behavior	Participation in normative social actions (protests, petitions, civil disobedience)
Contempt	Makes a statement about inherent moral superiority; activated by violation of common norms/values	Non-normative social actions (sabotage, violence, terrorism); devaluation of outgroup
Disgust	Helps to eliminate or repulse contaminated objects; aroused by violations of moral norms of	Violent actions against outgroup; devaluation; elimination; dehumanization

Emotion	Functional Perspective	Associated Actions
	purity/sanctity	
ANCODI Combination	Basic elements of hatred; activated simultaneously in different degrees; distinct from single emotions	Motivates hostility and violence; targets perceived as more threatening; increased willingness to attack

B. Identifying Vulnerable Communities in the US: Demographic and Socioeconomic Factors

Vulnerable populations are groups of individuals who face a heightened risk of health problems due to a variety of factors, including cultural, economic, ethnic, and geographic influences. This broad category encompasses diverse groups such as children, the elderly, the homeless, prisoners, low-income individuals, racial and ethnic minorities, and those lacking health insurance. Rural residents with limited access to healthcare are also considered part of this vulnerable demographic.

Vulnerability is a multifaceted concept, influenced by numerous interacting factors such as age, education, ethnicity, gender, illness, and income. It can be further compounded by residential location, socioeconomic status, and any physical or mental limitations an individual may have. Furthermore, significant life events, including abuse, neglect, lack of education, or poor nutrition during early life, can predispose individuals to later physical and social vulnerabilities, such as chronic illnesses, drug and alcohol dependency, homelessness, and incarceration.

Vulnerable populations are broadly categorized into groups facing physical (e.g., chronic illness, disability), psychological/mental (e.g., alcohol/drug dependency, mental health disorders), and social issues (e.g., abuse victims, homeless, incarcerated, immigrants, illiterate, poor, racial/ethnic minorities, non-English speakers, rural residents). The intersectionality of these factors amplifies vulnerability. For instance, climate change disproportionately affects socially vulnerable populations defined by income, educational attainment, race and ethnicity, and age, underscoring how multiple disadvantages can converge to create deeper susceptibility.

The combination and interaction of these vulnerabilities create a force multiplier effect, making communities exponentially more susceptible to exploitation. For example, a low-income, rural, ethnic minority community with limited access to education and healthcare presents a multi-layered vulnerability that is far more exploitable than any single vulnerability in isolation. This compounding of factors creates deeper grievances and reduces overall community resilience, making them prime targets for sophisticated influence operations. The presence of such layered vulnerabilities provides malign actors with multiple entry points and leverage points for cultivating ANCODI emotions and fostering destabilization.

Table 2: Key Demographic and Socioeconomic Vulnerabilities in US Communities

Category of Vulnerability	Specific Indicators
Demographic	Children, Elderly, Racial/Ethnic Minorities, Immigrants/Refugees
Socioeconomic	Low Income, Low Educational Attainment, Homelessness, Prisoners/Former Prisoners, Illiterate/Uneducated
Geographic	Rural Residents with limited healthcare access
Psychological/Social	Individuals with Disabilities/Chronic Illnesses, Mental Health Issues, Drug/Alcohol Dependency, Victims of Abuse/Neglect,

Category of Vulnerability	Specific Indicators
	Non-English Speakers

III. Mechanisms of Exploitation: Micro-Targeting and Influence Operations

A. Psychological Vulnerabilities and Susceptibility to Manipulation

Individuals predisposed to holding extreme social, political, and religious attitudes, and who are likely to support violence in the name of ideology, often exhibit a specific psychological signature. This signature includes poorer working memory, slower "perceptual strategies" (the unconscious processing of changing stimuli), and tendencies toward impulsivity and sensation seeking. This particular combination of cognitive caution and impulsive personality traits is a predictor for the endorsement of violence in support of an ideological group. Subtle difficulties with complex mental processing may subconsciously steer individuals towards extreme doctrines that offer clearer, more defined explanations of the world, thereby increasing their susceptibility to toxic forms of dogmatic and authoritarian ideologies. Radicalization itself is defined as a process involving the development of extremist beliefs, emotions, and behaviors, which can manifest as non-violent pressure and coercion, or actions that deviate from societal norms and demonstrate contempt for life, freedom, and human rights. From a functional standpoint, radicalization represents an enhanced preparation for and accentuated engagement in intergroup conflict.

The pathway to radicalization is often initiated by perceptions of injustice and relative deprivation, frequently rooted in the belief that one's group is unfairly disadvantaged compared to others, even if empirical evidence does not fully support such claims. Humiliation, shame, and anger, particularly when experienced in response to self- or group-relevant grievances, are prominent emotions during the pre-radicalization phase. These emotions create a powerful desire to re-establish a positive self- or group-image and motivate attempts to hold perceived perpetrators of unjust actions accountable. Moreover, experiences of discrimination, social isolation, and exposure to social networks that reinforce extremist views can significantly increase the vulnerability of youth to recruitment by terrorist groups. Narratives of victimization and existential threats play a crucial role in this radicalization process, as they fuel individuals' fundamental need for belonging and their drive to defend their threatened identities.

A critical phase in this process is what is termed "cognitive opening." This describes a moment of heightened vulnerability where an individual, facing discrimination, socioeconomic crisis, or political repression, begins to question previously accepted beliefs and becomes receptive to new, often radical, ideologies. This is not merely about the existence of grievances, but about a specific window of receptivity where those grievances become a potent leverage point for external influence. Malign actors actively seek to identify or even create conditions that induce this "cognitive opening" to effectively insert their radicalizing narratives.

The ANCODI hypothesis provides a direct link to the process of dehumanization, noting that disgust specifically functions to enable the "elimination" and "dehumanization" of outgroups. The literature on radicalization further supports this, indicating that individuals often undergo a process of dehumanizing the "other" as a prerequisite for committing acts of violence against them. This establishes a clear causal relationship: the deliberate cultivation of ANCODI emotions, particularly disgust, serves as a psychological tactic to facilitate violence. By stripping the target group of their humanity, malign actors can effectively overcome the moral sanctions that would otherwise prevent aggression, thereby escalating emotional manipulation into violent action.

B. Digital Ecosystems: Social Media, Dark Web, and AI as Enablers

Digital platforms and advanced technologies serve as powerful enablers for micro-targeting and the amplification of ANCODI emotions. Disinformation attacks are increasingly viewed as a cyber threat due to the pervasive use of internet manipulation on social media. Digital tools such as bots, sophisticated algorithms, and advanced AI technologies, often combined with human influencers, are systematically employed to spread and amplify disinformation. This allows for the precise micro-targeting of specific populations on widely used online platforms, including Instagram, Twitter, Google, Facebook, and YouTube. Microtargeting involves the meticulous collection and analysis of personal data to craft highly specific messaging for advertising, marketing, and influence campaigns. The ultimate goal for adversaries is to destabilize the leadership and decision-making processes of federal institutions responsible for public protection, and to manipulate and exploit vulnerable segments of entire populations. This is achieved by encouraging new insider threats and reactivating old grievances through deception and reflexive control, a technique that subtly guides individuals to act as desired by the manipulator. Social media algorithms, designed to maximize user engagement, often unintentionally amplify and accelerate the spread of misleading content. Disinformation has a documented tendency to travel farther, faster, and more broadly than truthful information, a phenomenon potentially driven by its novelty and emotional intensity. Content that triggers strong emotions, particularly anger and fear, is significantly more likely to be shared.

The algorithmic amplification of ANCODI emotions represents a dangerous feedback loop. Disinformation campaigns explicitly leverage content designed to trigger powerful emotions such as fear and anger to increase engagement and facilitate wider dissemination. Given that social media algorithms are engineered to maximize user engagement, they inadvertently prioritize and promote emotionally charged ANCODI content. This leads to a broader reach and faster propagation of such narratives, which in turn intensifies the ANCODI emotions within the target audience. This is a critical mechanism for the "amplification" aspect of the user's query, transforming individual emotional responses into a collective, destabilizing force.

The digital landscape also facilitates the creation and reinforcement of "echo chambers." Microtargeting efforts increasingly utilize social media platforms and other online forums to establish these echo chambers, where extremist views are introduced and continually reinforced through propaganda and disinformation. This phenomenon further entrenches sectarian and political divisions within communities. The anonymity afforded by the internet has contributed to the widespread use of bots and fake accounts, which create a false impression of widespread consensus or popular opposition, thereby manipulating public perception. Criminal organizations, for instance, frequently use encrypted messaging applications and online gaming or chat platforms to reach young individuals. They employ coded language, memes, and gamified tasks to attract recruits, offering incentives such as money, status, or a sense of belonging.

The Darkweb, accessible only through specialized software like Tor, allows criminals to conduct illicit activities such as cybercrime, drug trafficking, and exploitation with a high degree of anonymity. The use of cryptocurrencies like Bitcoin further enables untraceable financial transactions, contributing to the increased use of the Darkweb for "crime-as-a-service". This hidden online environment functions as an e-commerce market, a communication platform, and a source of threat intelligence. Critically, the Darkweb also serves to promote terrorism and radicalism, directly undermining the security of individuals, communities, and the broader environment. During periods of heightened societal fear and anxiety, such as the COVID-19 pandemic, the Darkweb experienced increased usage for illegal goods and services, and actively promoted apprehension and conspiracy theories. Law enforcement agencies face persistent challenges in identifying potential threats and perpetrators on the Darkweb due to its multi-lingual, mixed-style, and covert communication characteristics.

Malign actors are increasingly leveraging AI to execute cyberattacks, conduct fraud, and create deepfakes for extortion and misinformation dissemination. This integration of AI fundamentally reshapes criminal operations, making them faster, more efficient, and significantly more difficult to detect or counteract. Generative AI, in particular, enables the rapid creation of high-quality, idiomatically correct synthetic text, images, and audio, which allows influence actors to expand their messaging and lend it a greater aura of credibility.

The reliance on these digital tools by both state-sponsored actors and criminal groups highlights a convergence of methods in the digital domain. Both types of malign actors extensively utilize social media, AI, and the dark web, employing similar tactics such as disinformation, fake personas, and micro-targeting. This indicates that the digital landscape has created a shared operational environment where the tools traditionally associated with statecraft (e.g., influence operations) and those of traditional crime (e.g., financial fraud, illicit recruitment) are becoming increasingly indistinguishable and mutually reinforcing. This blurring of lines complicates attribution and counter-efforts, as the same digital infrastructure can be repurposed for a diverse range of malign objectives, from political interference to organized crime.

IV. State-Sponsored Actors: Cultivating ANCODI for Destabilization

A. Disinformation Campaigns and Narrative Amplification

State-sponsored disinformation campaigns are strategic deception efforts that employ media and internet manipulation to disseminate misleading information. Their primary objectives include confusing, paralyzing, and polarizing an audience. These campaigns utilize a range of general tactics, such as convincing target populations to believe factually incorrect information. A historical example includes the fraudulent claims by a British doctor in the 1990s about the MMR vaccine, which led to increased fear and a rise in preventable measles cases. More recently, repeated disinformation messages about election fraud were introduced years in advance of the 2020 United States presidential election to delegitimize its results.

Beyond spreading falsehoods, these campaigns also aim to undermine correct information by eroding belief in existing, accurate data. The MMR vaccine disinformation, for instance, ultimately fueled general fears about all vaccines, undermining a broad area of medical research. A key objective is the creation of uncertainty, intentionally designed to confuse and overwhelm people, whether targeting political opponents or "commercially inconvenient science." This tactic sows doubt to undermine support for opposing positions and prevent effective action. The "firehose of falsehood" model, exemplified by Russian propaganda, is characterized by high-volume and multichannel dissemination, continuous and repetitive messaging, and a deliberate disregard for objective reality and consistency. Its purpose is to "Deny, deflect, distract," thereby obscuring the truth.

A significant tactic involves undermining trust in critical institutions such as scientists, governments, and media, with real-world consequences. Disinformation campaigns around COVID-19 vaccines, for example, specifically targeted the vaccines, researchers, healthcare professionals, and policymakers, significantly impacting public trust and hindering effective responses to the virus. This strategy of "truth decay" goes beyond simply spreading falsehoods; it aims to erode the very concept of objective truth and the credibility of *all* information sources. This creates a deeper, more insidious strategy designed to foster a state of perpetual confusion and distrust, making populations more susceptible to any narrative, however outlandish, that aligns with their pre-existing biases or emotional state. This represents a direct assault on cognitive processing and critical thinking, which are foundational for a functioning democracy. Disinformation actors systematically cultivate networks of fake personas and websites, including fake expert networks that utilize inauthentic credentials (e.g., fake "experts," journalists, think tanks, or academic institutions) to lend undue credibility to their influence content and make it more believable. They also devise or amplify conspiracy theories by generating narratives that align with a conspiracy worldview, increasing the likelihood that the narrative will resonate with the target audience. "Astroturfing" and "flooding" are tactics that involve posting overwhelming amounts of content with the same or similar messaging from multiple inauthentic accounts. This practice creates the false impression of widespread grassroots support or opposition to a message while concealing its true origin. Furthermore, actors engage in spreading targeted content by producing tailored influence content designed to resonate with a specific audience based on their worldview and interests, often taking a "long game" approach to build trust and credibility over time. The increasing sophistication of these operations is augmented by malign actors leveraging AI to conduct hacks and fraud, create deepfakes for extortion and misinformation, and execute cyberattacks at massive scale, making criminal operations faster, more efficient, and alarmingly difficult to detect or counteract. Generative AI, in particular, enables the rapid creation of an endless supply of higher quality, more idiomatically correct text, thereby enhancing the ability of influence actors to expand their messaging and imbue it with a greater aura of credibility.

State-sponsored disinformation campaigns are designed to increase political polarization and alter public discourse, specifically aiming to amplify extreme positions and weaken a target society. In this context, domestic actors may also demonize political opponents. States with highly polarized political landscapes and low public trust are particularly vulnerable to these tactics. Foreign malign influence operations actively exploit perceived sociopolitical divisions to undermine confidence in U.S. institutions. These actors employ various methods, such as creating networks of fake online accounts to impersonate Americans, enlisting real individuals to wittingly or unwittingly promote their narratives, and utilizing proxies to launder their influence messages through a range of overt and covert channels. These operations consistently attempt to exacerbate existing social divides, amplify polarization, and push narratives that align with the nation-state's objectives, increasingly experimenting with generative AI to enhance these efforts. Disinformation commonly exploits existing societal fault lines of prejudice and polarization, frequently focusing on themes related to migrants and cultural diversity, gender and sexual diversity, public health and wellbeing, sustainability and climate, and urban planning. This represents the weaponization of identity politics. Foreign actors deliberately exploit "perceived sociopolitical divisions" and "existing societal fault lines of prejudice and polarization". This signifies a calculated strategy to exacerbate pre-existing tensions within communities, often along lines of identity such as race, ethnicity, religion, or political affiliation. By amplifying ANCODI emotions around these divisions, these actors transform internal societal differences into critical vulnerabilities, leading to fragmentation and conflict, which directly contributes to localized destabilization.

Table 3: State-Sponsored Disinformation Tactics and Their Impact on US Communities

Tactic	Description/Mechanism	Impact on US Communities
Convincing of Incorrect Information	Circulates beliefs difficult to fact-check; repeated false messages introduced years in advance	Leads to decisions counter to best interests; fuels vaccine hesitancy; delegitimizes election results
Undermining Correct Information	Erodes belief in existing, accurate information; fuels general fears about broad areas of research	Erodes belief in medical research; hinders effective public health responses
Creation of Uncertainty	Intentionally aims to confuse and overwhelm; sows doubt to undermine support and prevent action; "firehose of falsehood"	Prevents effective action; obscures truth; increases confusion and paralysis
Undermining Trust/Credibility	Questions underlying trust in scientists, governments, and media; attacks credibility of individuals/organizations	Impacts public trust in institutions; hinders effective responses (e.g., COVID-19); weakens rule of law
Cultivating Fake Personas/Websites	Creates networks of fake personas/websites with inauthentic credentials (e.g., fake experts, journalists)	Increases believability of messages; confuses audiences about authenticity
Amplifying Conspiracy Theories	Generates narratives aligning with conspiracy worldviews to resonate with target audience	Increases likelihood narrative will resonate; shapes entire worldview
Astroturfing/Flooding	Posts overwhelming amounts of similar content from inauthentic accounts; spams social media to shape narrative/drown out opposition	Creates false impression of widespread support/opposition; obscures true origin
Spreading Targeted Content	Produces tailored influence content likely to resonate with specific audience based on worldview/interests	Builds trust/credibility with target audience for future manipulation
AI/Deepfakes	Leverages AI for hacks, fraud, deepfakes for extortion/misinformation; creates synthetic text/image/audio	Makes criminal operations faster/more efficient/harder to detect; more convincing/harder-to-detect fakes
Exploiting Societal Divisions	Amplifies extreme positions; exacerbates existing social divides and polarization	Increases political polarization; weakens target society; sows division among Americans

B. Covert Operations and Proxy Networks

States strategically utilize non-state actors for covert subversion and malign networks to influence, manipulate, and obstruct affairs in other states while maintaining deniability. This approach makes it exceptionally difficult for targeted states to detect harmful activities, respond proactively, and accurately attribute operations to the foreign state. Methods employed include acting covertly through a third entity, such as the Russian Federation's use of the Pro-Russian nationalist group Night Wolves MC during the annexation of Crimea, which collected intelligence, distributed propaganda, and organized protests. States also deploy Private Military Corporations (PMCs), like the Russian Wagner Group, to deny and refute accusations of involvement in politically sensitive areas or conflict zones. Furthermore, exploiting criminal organizations is a common tactic, as these groups possess existing operations and networks within the target state. They can be leveraged for established smuggling networks, providing forged documents, engaging in financial crime schemes, or threatening, intimidating, pressuring, or harming strategically important individuals or groups for political purposes, as exemplified by the Iranian relationship with Hizballah. Plausible deniability is the cornerstone of these operations, enabling senior officials to deny knowledge or responsibility for actions committed by proxies. This is achieved by intentionally structuring power dynamics and chains of command loosely and informally enough to be disavowed if necessary.

The use of non-state actors by states signifies a "hybrid threat" model, blurring the lines between state and non-state aggression. States actively use criminal organizations and PMCs as proxies for covert operations. This is not merely outsourcing; it represents a strategic fusion of capabilities designed to achieve deniability and leverage existing illicit networks. This hybrid approach makes attribution and effective counter-responses significantly more challenging for targeted nations like the US, as the true source of destabilization is deliberately obscured.

The strategic objectives of these covert operations extend to influencing elections, undermining democratic institutions, and sowing discord within the target society. Foreign malign influence (FMI) activities often involve multiple actors, including foreign government officials, intelligence services, cyber actors, criminal groups, state-run media organizations, and social media actors. These malign influence agents frequently conceal their true affiliations to appear as legitimate U.S. citizens, trustworthy news sources, or benevolent participants in American institutions and processes. The overarching aim of FMI is to sow division among Americans, weaken confidence in democratic institutions and processes, or influence U.S. policy decisions in favor of a foreign actor's interests. A notable example is the Russian Internet Research Agency (IRA), which spent thousands on social media advertisements to influence the 2016 US presidential election, confuse the public, and sow discord, specifically targeting Mexican Americans and African Americans to foster mistrust and discourage voter turnout. Disinformation campaigns often intensify and peak just before elections, with automated bots triggering cascades of false information.

The repeated emphasis on "sowing division," "undermining confidence in democratic institutions," and "polarizing an audience" indicates a long-term strategic goal that transcends immediate political outcomes. This is a systematic effort to erode the foundational elements of a democratic society by exploiting its inherent freedoms, such as freedom of speech, to create internal fragility and diminish the capacity for collective action. This ultimately renders the society more susceptible to radicalization and external control.

C. Case Studies: Election Interference and Societal Polarization

Russian influence operations have been a prominent example of state-sponsored efforts to destabilize US communities. The Justice Department has actively disrupted covert Russian government-sponsored foreign malign influence operations that leveraged fabricated influencers, AI-generated content, paid social media advertisements, and social media accounts to direct internet traffic to cybersquatted and other deceptive domains. Russian companies, including Social Design Agency (SDA), Structura National Technology, and ANO Dialog, operating under the direct control of the Russian Presidential Administration, have been implicated in directing disinformation and state-sponsored narratives as part of campaigns to influence U.S. Presidential Elections, including the 2024 election cycle. The FBI has explicitly exposed these attempts, seizing 32 internet domains covertly used to spread foreign malign influence, thereby affirming Russia's ongoing status as a significant foreign threat to U.S. elections and society. Russia's efforts to influence the 2016 U.S. presidential election were characterized by a "significant escalation in directness, level of activity, and scope of effort," with the explicit aim of undermining public faith in the U.S. democratic process. Researchers have uncovered instances of Russian Federation-linked proxy news sites, such as "D.C. Weekly" and "New York News Daily," masquerading as legitimate U.S. local news outlets, which blended actual news reports with Russian disinformation. Russia has a long history of employing influence and coercion tactics, and now exploits America's societal divisions with disinformation to amplify discord and undermine its institutions, even extending these efforts to public health crises.

The Russian influence operations during the COVID-19 pandemic highlight a critical evolution beyond traditional electoral interference. By exploiting public health crises with disinformation, these actors weaponize fear and uncertainty (ANCODI) around vital public services. This demonstrates a capacity to generate an "infodemic" that directly impacts public safety and erodes trust in government responses, thereby contributing significantly to societal destabilization. This broader strategic aim seeks to undermine the state's ability to govern effectively and maintain social order.

Chinese influence operations, while distinct from Russia's, also pose a significant threat to US communities. A primary objective of PRC influence operations in the United States is to expand support for PRC interests among state and local leaders, leveraging these relationships to pressure Washington for policies more favorable to Beijing. The PRC recognizes the relative independence of U.S. state and local leaders and seeks to use them as proxies to advocate for national U.S. policies that align with Beijing's objectives. These influence operations are often deceptive and coercive, with seemingly benign business opportunities or people-to-people exchanges masking underlying PRC political agendas. The PRC systematically collects and analyzes personally identifiable information (PII) on U.S. state and local leaders and their close associates to identify potential opportunities and targets for influence. Pro-Beijing protests observed around Taiwanese president Tsai Ing-wen's transit through New York and Los Angeles in early 2023 serve as a clear illustration of United Front dynamics and tactics. These events involved overseas Chinese organizations and U.S. anti-war groups, with reports suggesting that the Chinese government financially incentivizes overseas Chinese individuals to participate in these protests.

The strategic focus of Chinese influence operations on subnational entities, such as state and local leaders and city-to-city partnerships , represents a "soft power" destabilization tactic. This approach is a "long game" strategy aimed at building dependencies and leveraging local interests to indirectly influence national policy and sow discord at a grassroots level. While these efforts may be less immediately disruptive than direct cyberattacks, they can have a cumulative corrosive effect on democratic integrity and social cohesion over time, as local decision-making processes become subtly influenced by foreign interests.

V. Criminal Actors: Exploiting Vulnerabilities for

Radicalization and Control

A. Recruitment and Grooming Tactics

Organized criminal groups systematically exploit vulnerable young people and adults for their illicit gains, often involving serious and organized criminality. A common method of control is debt exploitation, where young individuals become indebted to gangs and are then coerced into criminal activities to repay these debts. Gang membership frequently cultivates strong feelings of loyalty and belonging among its members, which is then leveraged as a powerful grooming mechanism to exploit individuals into participating in gang-related activities, including violence and drug dealing. Gangs strategically offer a sense of protection and status, appealing particularly to vulnerable youth who may suffer from low self-worth, unemployment, or academic failure and are seeking recognition or a place to excel. The allure of gang activity, characterized by excitement, danger, violence, and expressions of cultural biases, combined with the acceptance provided by fellow gang members, fulfills a critical need for social support and community involvement often absent in the lives of young male gang members.

The provision of "belonging," "family," and "social support" by gangs to vulnerable youth indicates that criminal actors exploit a fundamental human need for connection and identity. This is particularly effective for individuals experiencing social isolation or dysfunctional family environments. By offering a pseudo-family structure, gangs can then leverage loyalty and conformity to coerce individuals into criminal activity, effectively transforming a social vulnerability into a pathway for radicalization into a criminal lifestyle.

Organized crime groups employ psychological manipulation to influence the behavior of individuals and groups. This includes tactics such as persuasion and coercion to recruit new members or enforce loyalty, and the strategic use of intimidation and violence to control territory or markets. Within the hierarchical structures prevalent in many gangs, younger members often feel immense pressure to participate in violent or criminal acts as a means of "proving" their loyalty and ascending in status within the group. This participation is often driven by a deep-seated fear of other gang members or a strong desire to conform to the established culture of violence and criminality that defines gang life.

Both young men and women, particularly girls, face significant risks of sexual exploitation within these groups. Girls are frequently viewed as objects of status and power within the gang, and may be coerced into sexual activity with male gang members, or sexual acts may be used as a form of repayment for drug debts. In some extreme instances, rape and sexual assault are even employed as weapons against rival gangs. A specific tactic known as "county lines" drug dealing involves gangs exploiting vulnerable individuals or children to transport and sell drugs across county boundaries, thereby reducing the risk of detection for the core gang members. Similarly, "cuckooing" is a practice where gangs target vulnerable adults and take over their premises to distribute Class A drugs. The inherent difficulty of leaving a gang further perpetuates this cycle of exploitation, as many gangs issue explicit threats of violence against members who express a desire to leave, creating a coercive environment that traps individuals in criminal activity.

The tactics employed by criminal organizations, such as debt exploitation, sexual exploitation, coercion, and threats of violence for attempting to leave , illustrate a systematic process of entrapment. Initial perceived benefits, such as belonging, status, or financial gain, quickly transition into control maintained through fear and debt. This makes it increasingly difficult for exploited individuals to escape the criminal enterprise. This systematic process is a deliberate strategy to maintain control over vulnerable individuals, transforming them from passive targets of exploitation into active agents of criminal destabilization, which constitutes a form of radicalization into a criminal lifestyle.

B. Financial Exploitation and Market Distortion

The financial impact of organized crime extends far beyond direct monetary losses, actively distorting legitimate markets and undermining national security. Organized criminal groups (OCGs) deeply embed themselves within the legal economy, exploiting legitimate systems such as logistics chains, financial networks, shell companies, and digital platforms to conduct their operations, launder illicit profits, and mask illegal activities across diverse sectors including construction, retail, finance, and energy. This infiltration creates unfair competition for legitimate businesses, which are frequently extorted or forced out of the market due to the illicit advantages held by criminal enterprises.

Transnational organized crime (TOC) groups engage in a vast array of criminal activities, including drug trafficking, human trafficking, money laundering, firearms trafficking, illegal gambling, extortion, the creation and sale of counterfeit goods, wildlife and cultural property smuggling, and cybercrime. White-collar crimes, while non-violent in nature, such as fraud, embezzlement, insider trading, money laundering, bribery, and cybercrime, can lead to substantial financial losses for individuals, corporations, and entire economies. These losses can often dwarf the economic damage caused by more traditional forms of crime. Beyond immediate financial impact, white-collar crimes erode trust in economic and political institutions, exacerbate social inequality, and can even destabilize financial markets. High-profile cases, such as the Enron scandal or the Bernie Madoff Ponzi scheme, serve as stark reminders of the devastating ripple effects these crimes can have, affecting thousands of people and causing billions of dollars in damage.

Real estate fraud is a growing and sophisticated target for criminal actors, with fraudsters executing transactions with increasing speed and complexity. The consequences of real estate fraud extend beyond immediate financial losses, creating a ripple effect that can destabilize the industry, diminish public trust, and impede economic progress. Mortgage fraud, specifically, can disrupt the market by artificially inflating property values. Illicit financial flows (IFF) stemming from terrorism financing, human or drug trafficking, and other criminal activities are frequently moved and transferred through the U.S. financial system. These IFFs can result in destabilizing "hot money" flows, banking crises, ineffective revenue collection, broader governance weaknesses, and reputational risks for international financial centers. Market manipulation, encompassing tactics like "pump and dump" schemes, "spoofing," and insider trading, involves intentionally distorting financial markets for personal gain. This leads to increased prices for consumers, reduced market confidence, and unfair trading conditions, ultimately harming the broader economy.

The financial crimes perpetrated by criminal actors, including various forms of fraud, money laundering, and market manipulation, do not merely extract wealth; they actively "distort markets," "erode trust in institutions," and "contribute to social inequality". This creates a vicious economic feedback loop: economic destabilization leads to increased vulnerability within communities, which in turn provides more opportunities for criminal exploitation. This further erodes public trust and exacerbates existing societal divisions. This is a direct pathway to community destabilization, as economic hardship fuels social unrest and increases susceptibility to radical narratives, thereby creating a fertile ground for the cultivation of ANCODI emotions.

C. Dark Web Operations and Cybercrime

The Darkweb, a segment of the deep web, is exclusively accessible through specialized computer software such as Tor, and is extensively utilized for illegal activities including cybercrime, drug trafficking, and various forms of exploitation. Technological advancements, particularly the widespread adoption of Bitcoin and other cryptocurrencies, enable criminals to conduct these activities with a high degree of anonymity, leading to a significant increase in Darkweb usage. The Darkweb is widely recognized for fueling "crime-as-a-service," providing illicit capabilities and resources to a global network of criminals. It functions as a clandestine e-commerce market, a secure communication platform, an enabler for cybercrimes and untraceable financial transactions, and a source of threat intelligence for malign actors. Critically, the Darkweb also actively promotes terrorism and radicalism, directly sabotaging the security of individuals, communities, and the broader environment. During periods of heightened societal fear and anxiety, such as the COVID-19 pandemic, the Darkweb experienced a surge in use for illegal goods and services, and concurrently served as a platform for disseminating apprehension and conspiracy theories. Law enforcement agencies face persistent challenges in identifying signals of potential threats and pinpointing perpetrators on the Darkweb, largely due to its multi-lingual, mixed-style, and inherently covert communication characteristics.

Beyond merely facilitating traditional illicit trade, the Darkweb is explicitly linked to the "promotion of terrorism and radicalism" and the widespread dissemination of "conspiracy theories". This suggests that the Darkweb functions as a covert incubator for extremist ideologies, providing a secure and anonymous environment where radicalization narratives can take root and proliferate, particularly when societal fear and anxiety are elevated, as observed during a pandemic. The anonymity inherent in Darkweb operations enables the cultivation and amplification of ANCODI emotions without immediate accountability, making it a powerful tool for covert destabilization.

Ransomware, a type of malicious software, prevents users from accessing their computer files, systems, or networks and demands a ransom payment for their restoration. Ransomware attacks can lead to costly disruptions in operations and the irreversible loss of critical information and data. Recent ransomware attacks have severely impacted essential public services, crippling hospitals' ability to provide crucial care and disrupting public services in cities, causing significant damage to various organizations. Notable examples include attacks on the Los Angeles Superior Court, which effectively shut down the nation's largest trial court system, and attacks on Tri-City Medical Center and Singing River Health System, which disrupted hospital operations, forced ambulance diversions, and compromised the personal health information of hundreds of thousands of individuals. These attacks are not merely financial crimes; they pose a national security issue due to their capacity to disrupt vital services, cause substantial financial losses, facilitate data theft, and even lead to loss of life. State and local governments, businesses, schools, and hospitals across the U.S. continue to face persistent threats from ransomware and other malware attacks.

While financial fraud by criminal organizations indirectly contributes to destabilization, ransomware attacks on critical infrastructure such as hospitals, court systems, and other public services represent a *direct* form of localized destabilization. By disrupting essential services, these attacks create immediate chaos, severely erode public trust in governance, and can directly impact public safety and well-being. This creates an environment ripe for the amplification of ANCODI emotions, directed against perceived system failures or external threats, thereby accelerating societal fragmentation.

Table 4: Criminal Actor Exploitation Tactics and Societal Impacts

Tactic Category	Specific Tactics/Mechanisms	Societal Impact on US Communities
Recruitment & Grooming	Exploiting economic insecurity, social isolation, desire for belonging/status; persuasion, coercion, intimidation, sexual exploitation, debt bondage; "county lines" drug dealing; "cuckooing"	Entrapment of vulnerable individuals; increased criminal activity; breakdown of social norms; climate of fear; erosion of trust within communities; increased violence
Financial Exploitation & Market Distortion	Embedding in legal economy; unfair competition; illicit financial flows (ML/TF/PF); real estate fraud; investment fraud; market manipulation (pump & dump, spoofing, insider trading)	Distortion of markets; increased costs for goods/services; erosion of trust in economic/political institutions; social inequality; banking crises; loss of tax revenues; reduced consumer spending; economic instability
Dark Web Operations & Cybercrime	Anonymous illicit activities (cybercrime, drug trafficking, exploitation) via Tor/cryptocurrencies; "crime-as-a-service"; promotion of terrorism/radicalism; spread of conspiracy theories; ransomware attacks on critical infrastructure	Sabotage of security; public health risks (e.g., illicit vaccine trade); disruption of vital services (hospitals, courts); financial loss; data theft; erosion of public trust in governance; increased fear/anxiety

VI. Conclusions

The micro-targeting of Anger, Contempt, and Disgust (ANCODI) emotions in vulnerable US communities by both state-sponsored and criminal actors represents a sophisticated and evolving threat to national security and social cohesion. The analysis demonstrates a clear strategic convergence in the methods employed by these diverse malign entities. Both state and criminal actors exploit pre-existing demographic and socioeconomic vulnerabilities, leveraging digital ecosystems to amplify emotionally charged narratives that foster localized destabilization and radicalization.

State-sponsored actors, such as Russia and China, deploy advanced disinformation campaigns involving fake personas, proxy media, and AI-generated content to sow division, undermine trust in democratic institutions, and influence political processes. Their objectives extend beyond immediate electoral outcomes to a long-term erosion of the foundational elements of democratic society, often weaponizing existing societal fault lines and even public health crises to create an "infodemic" of confusion and distrust. The strategic use of non-state proxies provides deniability, making attribution and response challenging.

Criminal actors, including organized crime groups and gangs, similarly exploit vulnerabilities like economic insecurity, social isolation, and the desire for belonging. They employ psychological manipulation, coercion, and intimidation tactics to recruit and control individuals, radicalizing them into criminal lifestyles. Their financial exploitation, through various frauds and market distortions, not only generates illicit profits but also systematically erodes trust in economic institutions and exacerbates social inequality, creating a fertile ground for further unrest. Furthermore, dark web operations and cybercrime, particularly ransomware attacks on critical infrastructure, directly destabilize communities by disrupting essential services, leading to immediate chaos and further diminishing public trust.

The common thread across these threats is the deliberate cultivation of ANCODI emotions. Anger, contempt, and disgust are not merely byproducts but central to the strategic objectives, serving as psychological catalysts for escalating hostility, dehumanization, and ultimately, violence. The digital environment, with its algorithmic amplification and capacity for creating echo chambers, significantly accelerates and expands the reach of these emotionally manipulative campaigns. The blurring of lines between state and non-state actors, and the convergence of their tactics, underscore the complexity of this threat landscape. Addressing this challenge requires a comprehensive, multi-faceted approach that recognizes the deep psychological underpinnings of radicalization and the intricate interplay of digital and socio-economic vulnerabilities.

Works cited

1. Emotion and aggressive intergroup cognitions: The ANCODI hypothesis - PubMed, https://pubmed.ncbi.nlm.nih.gov/27405292/ 2. Emotion and aggressive intergroup cognitions: The ANCODI hypothesis - ResearchGate, https://www.researchgate.net/publication/305276986_Emotion_and_aggressive_intergroup_cognitions_The_ANCODI_hypothesis_The_ANCODI_Hypothesis 3. Intergroup emotions and political aggression: The ANCODI hypothesis - Sydney Symposium of Social Psychology, https://sydneysymposium.unsw.edu.au/2014/chapters/FrankSSSP2014.pdf 4. Vulnerable populations | EBSCO Research Starters, https://www.ebsco.com/research-starters/political-science/vulnerable-populations 5. Social Vulnerability Report | US EPA - Environmental Protection Agency (EPA), https://www.epa.gov/cira/social-vulnerability-report 6. Psychological 'signature' for the extremist mind uncovered - University of Cambridge, https://www.cam.ac.uk/stories/extremistmind 7. Psychological Mechanisms Involved in Radicalization and Extremism. A Rational Emotive Behavioral Conceptualization - Frontiers, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2019.00437/full 8. Understanding Political Radicalization: The Two-Pyramids Model - American Psychological Association, https://www.apa.org/pubs/journals/releases/amp-amp0000062.pdf 9. (PDF) Emotions in Violent Extremism - ResearchGate, https://www.researchgate.net/publication/378317108_Emotions_in_Violent_Extremism 10. Tackling Terrorists' Exploitation of Youth - the United Nations, https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/05/report/tackling-terrorists-exploitation-of-youth/Tackling-Terrorists-Exploitation-of-Youth.pdf 11. Understanding Violent Extremism: The Social Psychology of Identity and Group Dynamics, https://arabcenterdc.org/resource/understanding-violent-extremism-the-social-psychology-of-identity-and-group-dynamics/ 12. Preventing Violent Extremism: A Review of the Literature - Taylor & Francis Online, https://www.tandfonline.com/doi/full/10.1080/1057610X.2018.1543144 13. Disinformation attack - Wikipedia, https://en.wikipedia.org/wiki/Disinformation_attack 14. MICROTARGETING UNMASKED: - Secret Service, https://www.secretservice.gov/sites/default/files/reports/2023-08/asu-tc-micro-targeting-report_final.pdf 15. Information Pandemic: A Critical Review of Disinformation Spread on Social Media

and Its Implications for State Resilience - MDPI, https://www.mdpi.com/2076-0760/13/8/418 16. Three things to know about foreign disinformation campaigns, https://washingtondc.jhu.edu/news/three-things-to-know-about-foreign-disinformation-campaigns/ 17. What Is a Disinformation Campaign? | CrowdStrike, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/disinformation-campaign/ 18. Fanning the Flames: How Misinformation on Social Media Exacerbates Community Tensions - The London School of Economics and Political Science, https://www.lse.ac.uk/geography-and-environment/research/social-media-and-crisis-of-urban-inequality-blog/fanning-the-flames-how-misinformation-on-social-media-exacerbates-community-tensions 19. How states use non-state actors: A modus operandi for ... - Hybrid CoE, https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_15_Non-state-Actors.pdf 20. Violence-as-a-Service Providers Increasingly Recruit Minors to Carry Out Harmful Acts, https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/august/Violence-as-a-Service-Recruits-Young-People/ 21. Darkweb research: Past, present, and future trends and mapping to sustainable development goals - PMC - PubMed Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC10695971/ 22. What Are Social Engineering Attacks? A Detailed Explanation | Splunk, https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html 23. The Rise of AI-Enabled Crime: Exploring the evolution, risks, and responses to AI-powered criminal enterprises - TRM Labs, https://www.trmlabs.com/resources/blog/the-rise-of-ai-enabled-crime-exploring-the-evolution-risks-and-responses-to-ai-powered-criminal-enterprises 24. Combatting Deepfakes - Future of Life Institute, https://futureoflife.org/project/combatting-deepfakes/ 25. Homeland Threat Assessment 2024 - Homeland Security, https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf 26. The Dark Art of PSYOP in Organized Crime - Number Analytics, https://www.numberanalytics.com/blog/the-dark-art-of-psyop-in-organized-crime 27. Office of Public Affairs | Justice Department Disrupts Covert Russian ..., https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence 28. SECURING ELECTION INFRASTRUCTURE AGAINST THE TACTICS OF FOREIGN MALIGN INFLUENCE OPERATIONS | DNI.gov, https://www.dni.gov/files/FMIC/documents/products/Securing-Election-Infrastructure-Against-The-Tactics-Of-Foreign-Malign-Influence-Operations-Apr2024.pdf 29. Tactics of Disinformation - CISA, https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf 30. Disinformation in the City Response Playbook - German Marshall Fund, https://www.gmfus.org/sites/default/files/2024-08/Disinformation%20in%20the%20City%20RESPONSE%20PLAYBOOK.pdf 31. DISINFORMATION IN THE CITY RESPONSE PLAYBOOK - The University of Melbourne, https://www.unimelb.edu.au/__data/assets/pdf_file/0006/5060724/Disinformation-in-the-City-Reponse-Playbook_compressed-1.pdf 32. Plausible deniability - Wikipedia, https://en.wikipedia.org/wiki/Plausible_deniability 33. A New International Approach to Beating Serious and Organised Crime - Tony Blair Institute, https://institute.global/insights/public-services/a-new-international-approach-to-beating-serious-and-organised-crime 34. FMI Primer - DNI.gov, https://www.dni.gov/files/FMIC/documents/products/04-25-24_Report_FMI-Primer-Public-Release.pdf 35. Evaluation of the US Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to US Elections, https://oig.justice.gov/sites/default/files/reports/24-080.pdf 36. Ex-CIA analyst challenges

Trump's attempt to discredit Russian election interference probe, https://www.pbs.org/newshour/show/ex-cia-analyst-challenges-trumps-attempt-to-discredit-russian-election-interference-probe 37. Foreign Disinformation: Defining and Detecting Threats | U.S. GAO, https://www.gao.gov/products/gao-24-107600 38. Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2420792/social-media-weaponization-the-biohazard-of-russian-disinformation-campaigns/ 39. 1 July 2022 Overview For decades, a broad range of entities in China have forged ties with government and business leaders at th - DNI.gov, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/PRC_Subnational_Influence-06-July-2022.pdf 40. China's Political Influence Tactics and Transnational Repression Activities Against Taiwan - CECC.gov, https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/evo-media-document/wong-written-testimony-073125.pdf 41. Gang Activity, Youth Violence and Criminal Exploitation..., https://gloucestershirescp.trixonline.co.uk/chapter/gang-activity-youth-violence-and-criminal-exploitation-affecting-children 42. Gangs - Preventing Exploitation Toolkit, https://www.preventingexploitationtoolkit.org.uk/home/what-is-exploitation/what-is-vulnerability/gangs/ 43. Traits of Gang Members - Edmonton Police Service, https://www.edmontonpolice.ca/CommunityPolicing/OrganizedCrime/Gangs/TraitsofGangMembers 44. Gangs, violence and the role of women and girls: - Global Initiative Against Transnational Organized Crime, https://globalinitiative.net/wp-content/uploads/2017/04/TGIATOC-Gangs_-violence-and-the-role-of-women-and-girls-1837-web.pdf 45. Organized crime - Wikipedia, https://en.wikipedia.org/wiki/Organized_crime 46. Transnational Organized Crime - FBI, https://www.fbi.gov/investigate/transnational-organized-crime 47. Common White Collar Crimes: Understanding Their Impact | NU - National University, https://www.nu.edu/blog/common-white-collar-crimes/ 48. Real Estate Fraud Deconstructed: Themes and Classifications - International Journal of Research and Innovation in Social Science, https://rsisinternational.org/journals/ijriss/articles/real-estate-fraud-deconstructed-themes-and-classifications/ 49. Illicit Finance: Agencies Could Better Assess Progress in Countering Criminal Activity - GAO, https://www.gao.gov/products/gao-25-106568 50. Anti-Money Laundering and Combating the Financing of Terrorism, https://www.imf.org/en/Topics/Financial-Integrity/amlcft 51. How Market Manipulation Affects Consumers and Businesses - Leppard Law, https://federal-criminal.com/white-collar/how-market-manipulation-affects-consumers-and-businesses/ 52. Types of Illegal Stock Market Manipulation - Federal Criminal Defense Attorney, https://www.thefederalcriminalattorneys.com/stock-market-manipulation 53. Ransomware - FBI, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware 54. Ransomware Attack - What is it and How Does it Work? - Check Point Software, https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ 55. The Impact of Cyber Attacks on US Citizens | Rubrik, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-the-impact-of-cyber-attacks-on-us-citizens.pdf