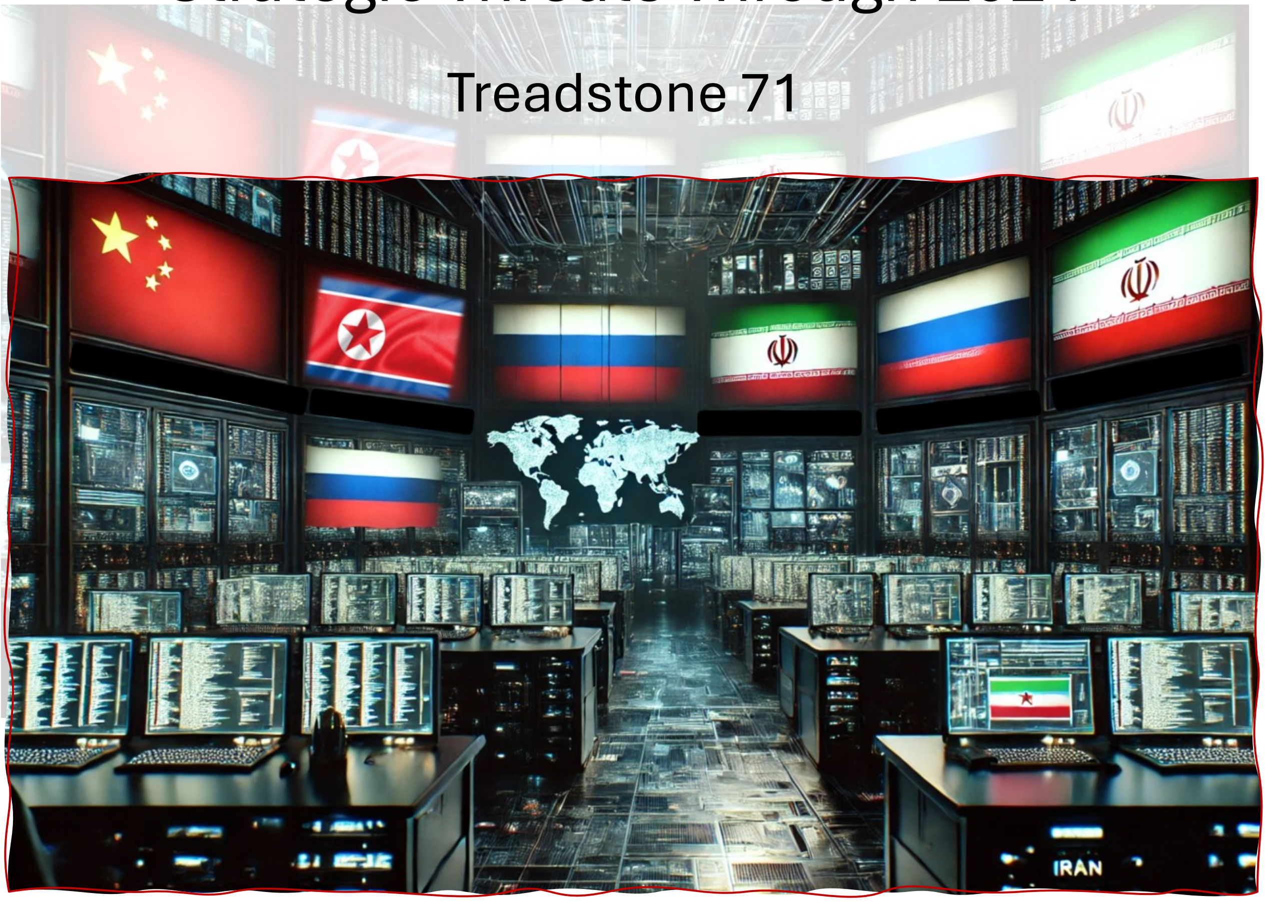
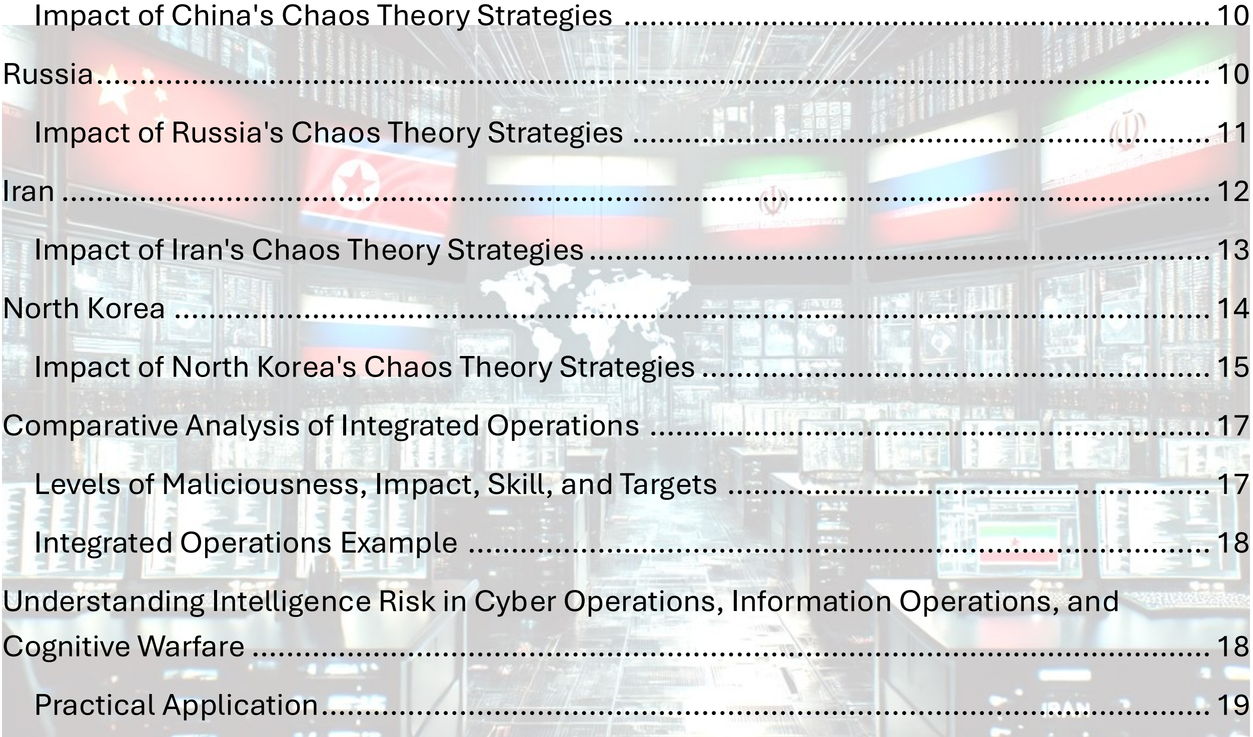
Cyber, Info Ops, and Cognitive Warfare from China, Iran, Russia, and North Korea

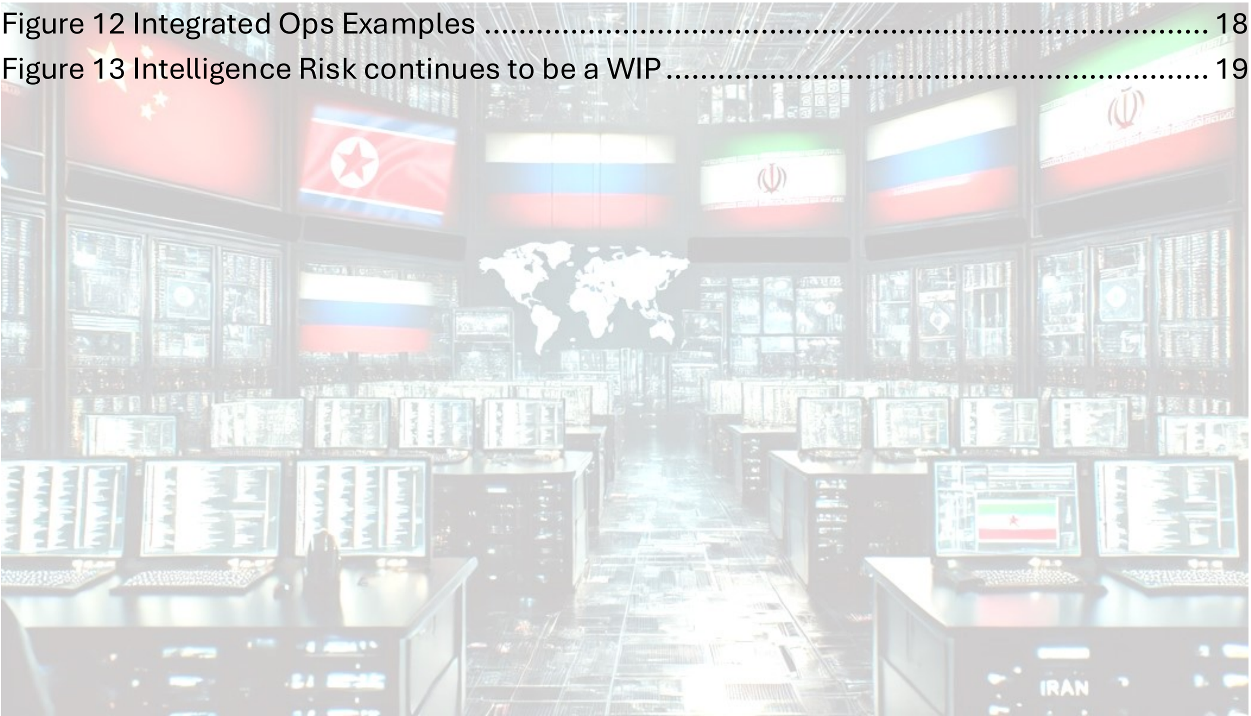
Strategic Threats Through 2024

Treadstone 71

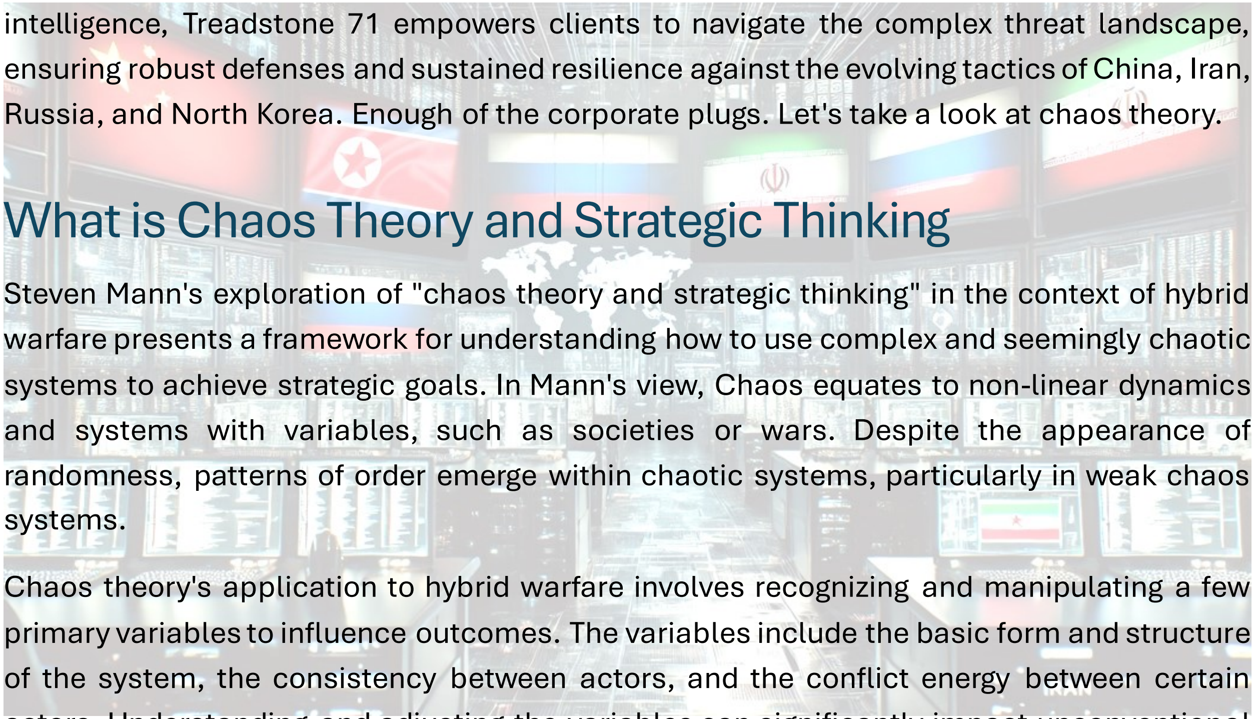


Contents




IRAN

Understanding and countering the actions of adversarial nations is paramount. China, Iran, Russia, and North Korea use sophisticated strategies that disrupt and destabilize Western societies, using cyber operations, information warfare, and cognitive manipulation. Organizations must stay vigilant and prepared to defend against these comprehensive and targeted threats. Treadstone 71 stands at the forefront of this battle, offering unparalleled training, consulting, and services designed to equip organizations with the knowledge and tools necessary to anticipate, detect, and counter the malicious activities of adversaries. Through comprehensive education, strategic consulting, and real-time intelligence, Treadstone 71 empowers clients to navigate the complex threat landscape, ensuring robust defenses and sustained resilience against the evolving tactics of China, Iran, Russia, and North Korea. Enough of the corporate plugs. Let's take a look at chaos theory.



What is Chaos Theory and Strategic Thinking

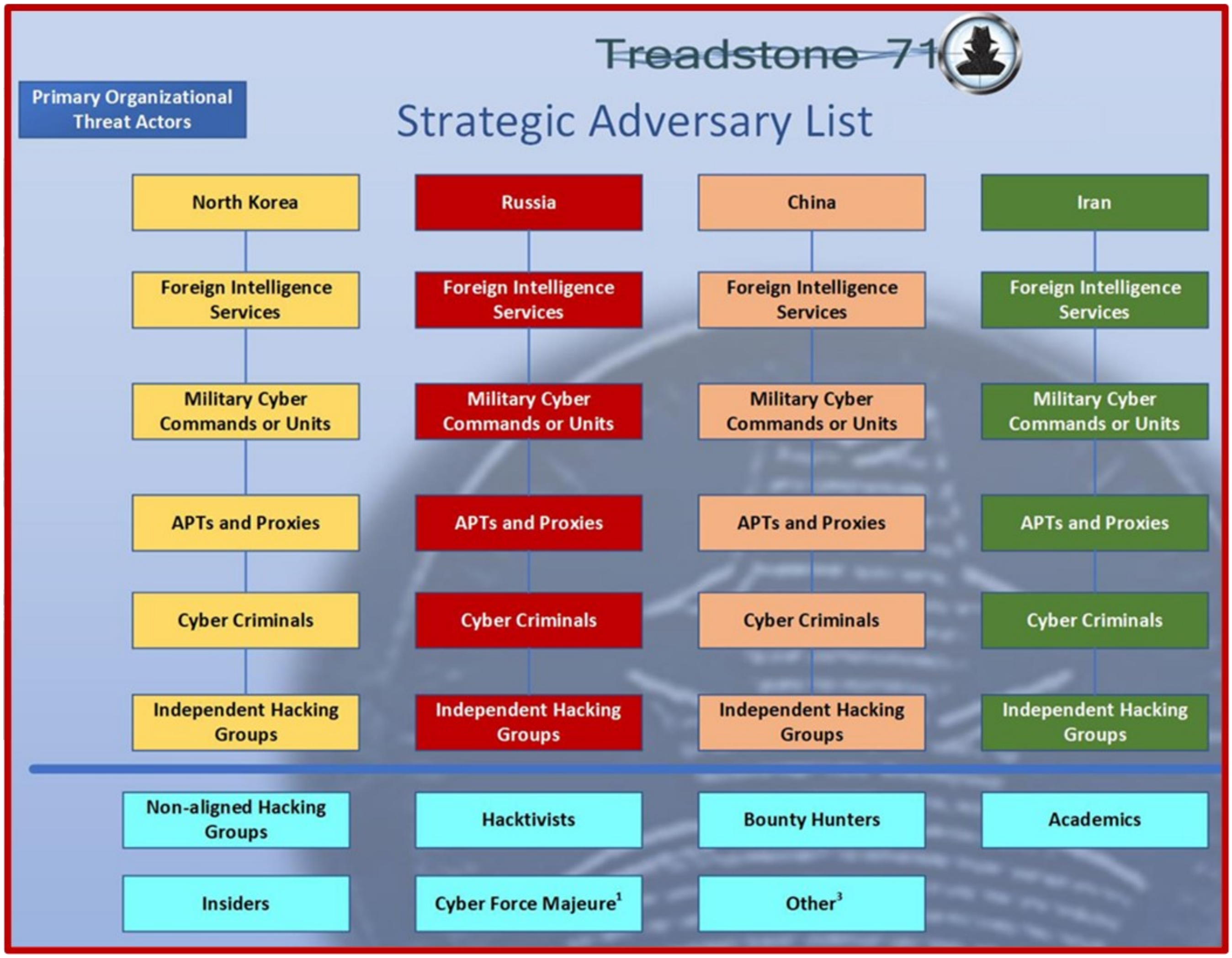
Steven Mann's exploration of "chaos theory and strategic thinking" in the context of hybrid warfare presents a framework for understanding how to use complex and seemingly chaotic systems to achieve strategic goals. In Mann's view, Chaos equates to non-linear dynamics and systems with variables, such as societies or wars. Despite the appearance of randomness, patterns of order emerge within chaotic systems, particularly in weak chaos systems.

Chaos theory's application to hybrid warfare involves recognizing and manipulating a few primary variables to influence outcomes. The variables include the basic form and structure of the system, the consistency between actors, and the conflict energy between certain actors. Understanding and adjusting the variables can significantly impact unconventional warfare and color revolutions.

For instance, the initial social situation in a target country is as crucial for revolution as the initial physical, military, and infrastructural conditions are for unconventional warfare. When all system components become sensitive, the conflict energy between actors becomes evident. Actors strategically manipulate conflict energy to achieve desired outcomes.

Mann proposes that strategic manipulation of "software" or individuals' ideological and cognitive frameworks is necessary to change the energy and conflict within a society. The manipulation resembles a virus in hacking, where ideology serves as a tool to alter human "software." The spreading of ideological "viruses" makes it possible to influence political feelings and ideas, transmitting new political thoughts and actions across various levels of society.

In hybrid warfare, creating and manipulating social networks is crucial. The formation of groups through social networks facilitates the spread of innovative ideas and ideologies. Once individuals adopt innovative ideas, they actively disseminate them to others, leading to a broader transmission of political change. The process is akin to the spread of a virus, where one infected individual can infect many others, creating a chain reaction of ideological and political shifts.



Treadstone 71

Primary Organizational Threat Actors

Strategic Adversary List

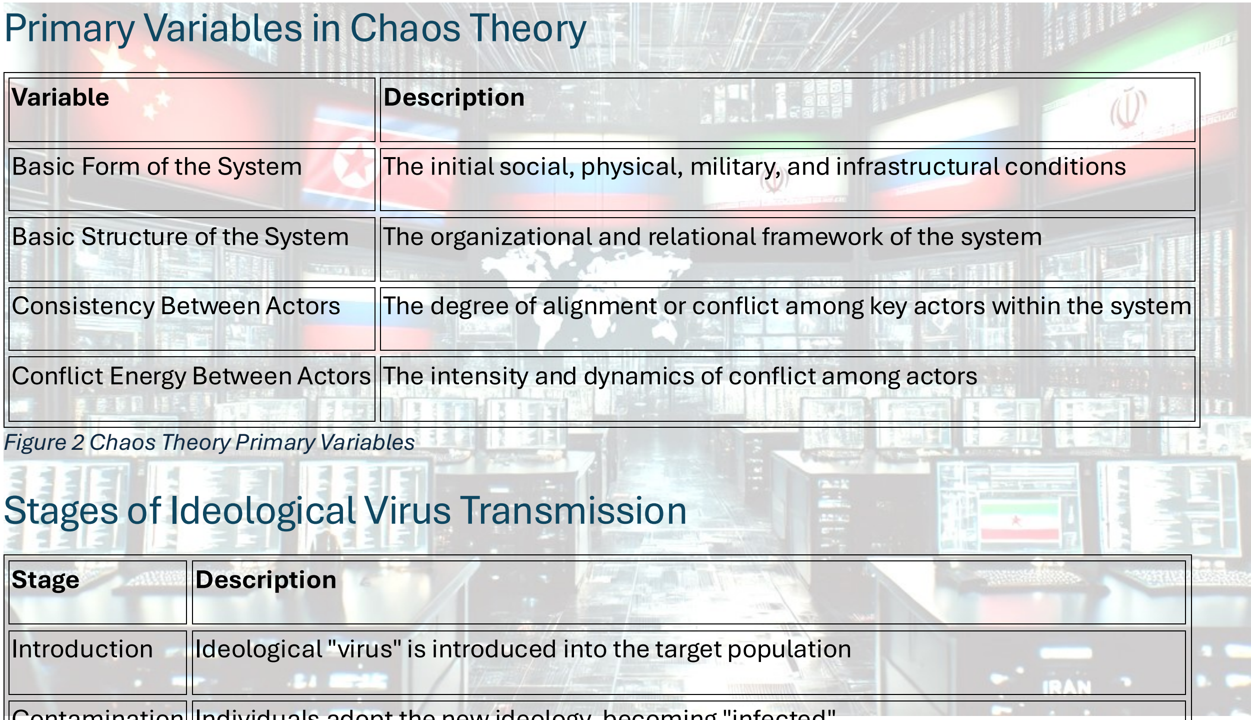
North Korea	Russia	China	Iran
Foreign Intelligence Services	Foreign Intelligence Services	Foreign Intelligence Services	Foreign Intelligence Services
Military Cyber Commands or Units	Military Cyber Commands or Units	Military Cyber Commands or Units	Military Cyber Commands or Units
APTs and Proxies	APTs and Proxies	APTs and Proxies	APTs and Proxies
Cyber Criminals	Cyber Criminals	Cyber Criminals	Cyber Criminals
Independent Hacking Groups	Independent Hacking Groups	Independent Hacking Groups	Independent Hacking Groups
Non-aligned Hacking Groups	Hacktivists	Bounty Hunters	Academics
Insiders	Cyber Force Majeure[1]	Other[3]	

Figure 1 Strategic Adversary List - Top 4

The strategic aspect of this approach lies in its ability to penetrate the five social circles of target citizens, using methods such as color revolutions to spread messages and achieve goals. By embedding ideological "viruses" into the social fabric, it becomes possible to win over compatible targets and gradually implement changes at various levels of society.

Understanding the patterns within Chaos allows for the development of strategies that advance national security interests by reducing or redirecting societal conflict energy. Hybrid warfare, therefore, involves a sophisticated interplay of cognitive warfare, information operations, and cyber operations. Cognitive warfare targets the minds of individuals, influencing their perceptions and beliefs. Information operations manipulate the flow of information to control narratives and shape public opinion. Cyber operations exploit technological vulnerabilities to achieve strategic objectives.

Tables or charts that can help illustrate these concepts include a breakdown of the primary variables in chaos theory, the stages of ideological virus transmission, and the interplay between cognitive, information, and cyber operations.



Primary Variables in Chaos Theory

Variable	Description
Basic Form of the System	The initial social, physical, military, and infrastructural conditions
Basic Structure of the System	The organizational and relational framework of the system
Consistency Between Actors	The degree of alignment or conflict among key actors within the system
Conflict Energy Between Actors	The intensity and dynamics of conflict among actors

Figure 2 Chaos Theory Primary Variables

Stages of Ideological Virus Transmission

Stage	Description
Introduction	Ideological "virus" is introduced into the target population
Contamination	Individuals adopt the new ideology, becoming "infected"
Transmission	Infected individuals actively spread the ideology to others
Proliferation	Widespread adoption of the ideology leading to significant political and social changes

Figure 3 Cognitive Warfare Virus Transmission

Interplay Between Cognitive, Information, and Cyber Operations

Operation Type	Target	Methods
Cognitive Warfare	Minds of individuals	Ideological manipulation, psychological operations, perception management
Information Operations	Public opinion	Propaganda, misinformation, narrative control
Cyber Operations	Technological vulnerabilities	Hacking, cyber-attacks, digital espionage

Figure 4 Interplay Based on Target and Methods

Mann's application of chaos theory to hybrid warfare offers a comprehensive strategy for manipulating complex systems to achieve strategic objectives, emphasizing the importance of cognitive, information, and cyber operations in modern conflict.

Adversarial Use

China, Iran, and Russia have increasingly applied chaos theory principles in their strategies against the US and NATO, exploiting non-linear dynamics to create uncertainty and destabilization. China's use of information operations and cyber warfare has aimed to undermine democratic processes and sow discord among NATO members. Recent disinformation campaigns targeting US elections involved spreading false narratives to polarize voters and erode trust in democratic institutions. The efforts extended to cyber-attacks on critical infrastructure, aiming to create vulnerabilities and demonstrate the capacity to disrupt Western societies.

Iran's approach has focused on exploiting regional conflicts and social divisions to challenge US influence in the Middle East. Through proxy groups and cyber capabilities, Iran has targeted US allies and interests, creating Chaos in already volatile regions. For example, Iran's support for militant groups in Iraq and Yemen has intensified conflicts, drawing US resources and attention away from broader strategic goals. Additionally, Iranian cyber-attacks on US government networks and private sector companies have aimed to steal sensitive information and disrupt operations, further contributing to a sense of instability.

Russia has employed a sophisticated blend of cognitive warfare, cyber operations, and information manipulation to weaken NATO cohesion and challenge US leadership. Russian disinformation campaigns have targeted various NATO countries, spreading conspiracy theories and fake news to deepen political divides and weaken public trust in governments. Cyber-attacks attributed to Russian state actors have focused on critical infrastructure, election systems, and media outlets, aiming to create Chaos and uncertainty. Russia's use of hybrid warfare in Ukraine exemplifies its strategy of blending conventional and unconventional tactics to achieve strategic objectives without triggering a full-scale military response.

The application of chaos theory by adversaries reveals a deliberate effort to exploit vulnerabilities in Western societies and institutions. By creating and amplifying Chaos, China, Iran, and Russia intend to weaken the strategic position of the US and NATO, forcing them to address multiple crises simultaneously and diverting attention from broader geopolitical ambitions.

Recent Examples and Impact

Country	**Strategy**	**Recent Example**	**Impact**
China	Information operations, cyber warfare	Disinformation campaigns during US elections, cyber-attacks on infrastructure	Polarization of voters, erosion of trust in democratic institutions
Iran	Regional conflict exploitation, cyber capabilities	Support for militant groups in Iraq and Yemen, cyber-attacks on US networks	Intensified regional conflicts, resource diversion, operational disruption
Russia	Cognitive warfare, hybrid warfare, cyber operations	Disinformation campaigns in NATO countries, cyber-attacks on critical infrastructure	Weakened NATO cohesion, political divides, uncertainty, and instability

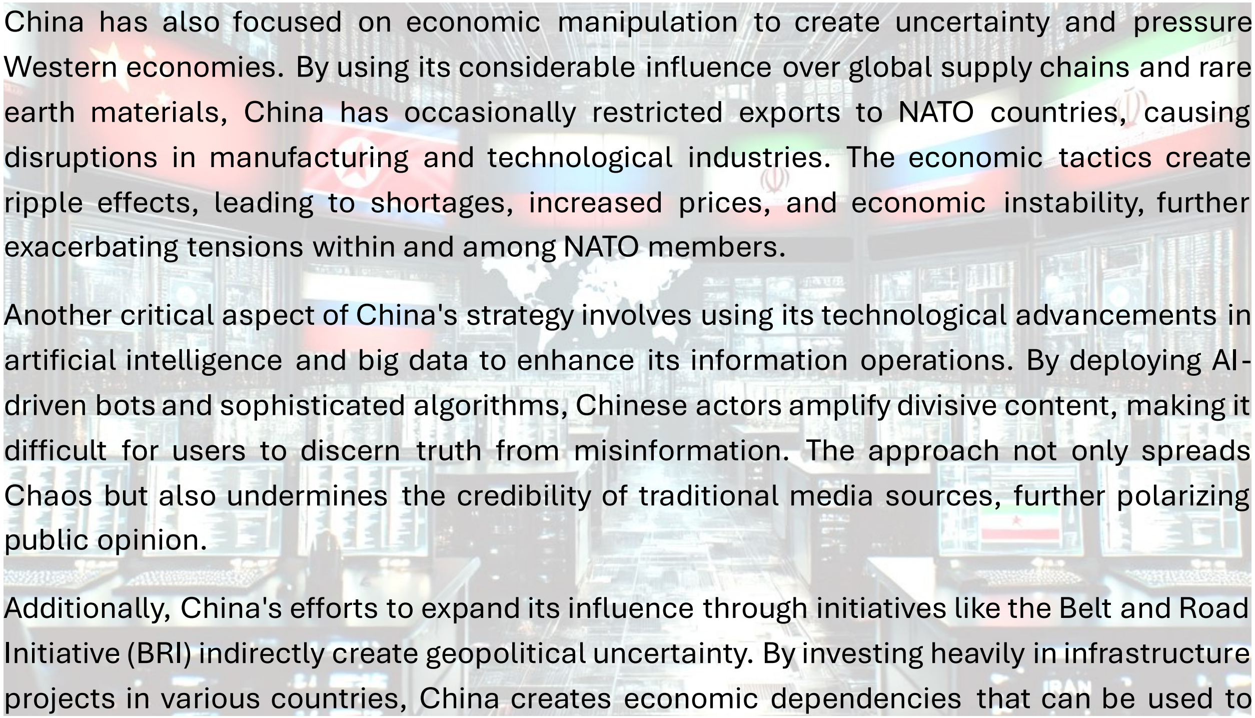
Figure 5 Recent Top 3 Country Examples

The actions underscore the strategic application of chaos theory by China, Iran, North Korea, and Russia in their efforts to destabilize and weaken Western adversaries.

China

China has strategically employed chaos theory against the US and NATO by targeting social and political stability through sophisticated information operations and cyber warfare. Recently, Chinese actors engaged in disinformation campaigns aimed at undermining public confidence in democratic processes, particularly during the US elections. By spreading false narratives and conspiracy theories through social media and other online platforms, Chinese operatives sought to polarize voters, create distrust in electoral outcomes, and amplify existing societal divisions.

Furthermore, Chinese cyber-attacks on critical infrastructure, including healthcare, energy, and communication networks, have increased in frequency and sophistication. The attacks disrupt essential services, create vulnerabilities, and demonstrate China's ability to destabilize Western societies. For instance, cyber-attacks attributed to Chinese hackers targeted US healthcare institutions during the COVID-19 pandemic, aiming to steal sensitive data and create Chaos in an already strained system. Such actions cause immediate disruptions and erode public trust in the government's ability to protect its citizens and maintain stability.



China has also focused on economic manipulation to create uncertainty and pressure Western economies. By using its considerable influence over global supply chains and rare earth materials, China has occasionally restricted exports to NATO countries, causing disruptions in manufacturing and technological industries. The economic tactics create ripple effects, leading to shortages, increased prices, and economic instability, further exacerbating tensions within and among NATO members.

Another critical aspect of China's strategy involves using its technological advancements in artificial intelligence and big data to enhance its information operations. By deploying AI-driven bots and sophisticated algorithms, Chinese actors amplify divisive content, making it difficult for users to discern truth from misinformation. The approach not only spreads Chaos but also undermines the credibility of traditional media sources, further polarizing public opinion.

Additionally, China's efforts to expand its influence through initiatives like the Belt and Road Initiative (BRI) indirectly create geopolitical uncertainty. By investing heavily in infrastructure projects in various countries, China creates economic dependencies that can be used to influence political decisions, often causing friction between those countries and NATO members. The strategy creates a complex web of economic and political entanglements, making it challenging for NATO to present a unified front against Chinese influence.

The comprehensive application of chaos theory by China against the US and NATO demonstrates attempts to destabilize and weaken Western societies. China's tactics span from information warfare and cyber operations to economic manipulation and geopolitical influence, designed to create uncertainty and exploit vulnerabilities in Western systems.

Impact of China's Chaos Theory Strategies

Strategy	Recent Example	Impact
Information operations	Disinformation during US elections	Polarization, distrust in democratic processes
Cyber warfare	Attacks on US healthcare during COVID-19	Disruptions, erosion of public trust
Economic manipulation	Restrictions on rare earth material exports	Manufacturing disruptions, economic instability
Technological advancements	AI-driven misinformation campaigns	Amplified divisive content, undermined media credibility
Geopolitical influence	Belt and Road Initiative investments	Economic dependencies, geopolitical friction with NATO members

Figure 6 Chinese Chaos Theory recent examples and impacts

China's strategic application of chaos theory against the US and NATO exploits and amplifies existing vulnerabilities, creating an environment of uncertainty and instability that undermines the West's ability to respond effectively to Chinese actions and policies.

Russia

Russia has applied chaos theory against the US and NATO by using a combination of disinformation campaigns, cyber operations, and geopolitical tactics to create uncertainty and destabilize Western societies. Russian actors have targeted democratic processes through sophisticated disinformation efforts. For example, during the 2016 US presidential election, Russian operatives spread false narratives and divisive content across social media platforms to polarize voters and undermine confidence in the electoral process. The approach has continued in subsequent elections, with Russian influence operations aiming to deepen societal divisions and erode trust in democratic institutions.

Cyber operations form a significant part of Russia's strategy. Russian state-sponsored hackers have targeted critical infrastructure in NATO countries, including power grids, financial systems, and communication networks. One notable incident involved the 2017 NotPetya malware attack, which caused widespread disruption across several countries, including Ukraine, a NATO partner. The attack resulted in billions of dollars in damages and highlighted the vulnerabilities in Western infrastructure. Such cyber-attacks intend to create Chaos, disrupt daily life, and demonstrate Russia's capability to inflict damage without direct military confrontation.

Russia has also engaged in hybrid warfare to achieve its strategic goals. The annexation of Crimea in 2014 exemplifies Russia's use of hybrid tactics, blending conventional military force with irregular warfare and information operations. Russian forces, often referred to as "little green men" due to their unmarked uniforms, operated alongside local militias and used propaganda to create a narrative of local support for the annexation. The approach allowed Russia to achieve its objectives while maintaining a degree of plausible deniability and creating confusion among NATO members about the appropriate response.

Additionally, Russia has exploited economic and political vulnerabilities in NATO countries to exert influence and create discord. Russia has pressured European countries dependent on Russian energy by controlling energy supplies, particularly natural gas. The economic manipulation creates tensions within NATO, as member states struggle to balance their energy needs with the political imperative to counter Russian aggression. For instance, the Nord Stream 2 pipeline project has been a source of contention within NATO, with members viewing it as a threat to European energy security and others prioritizing economic benefits.

Russia's use of information warfare extends beyond elections and political processes. Russian media outlets, such as RT and Sputnik, spread disinformation and propaganda to shape public opinion and sow discord in NATO countries. The media campaigns often promote conspiracy theories and false narratives, aiming to undermine trust in government institutions and exacerbate societal divisions.

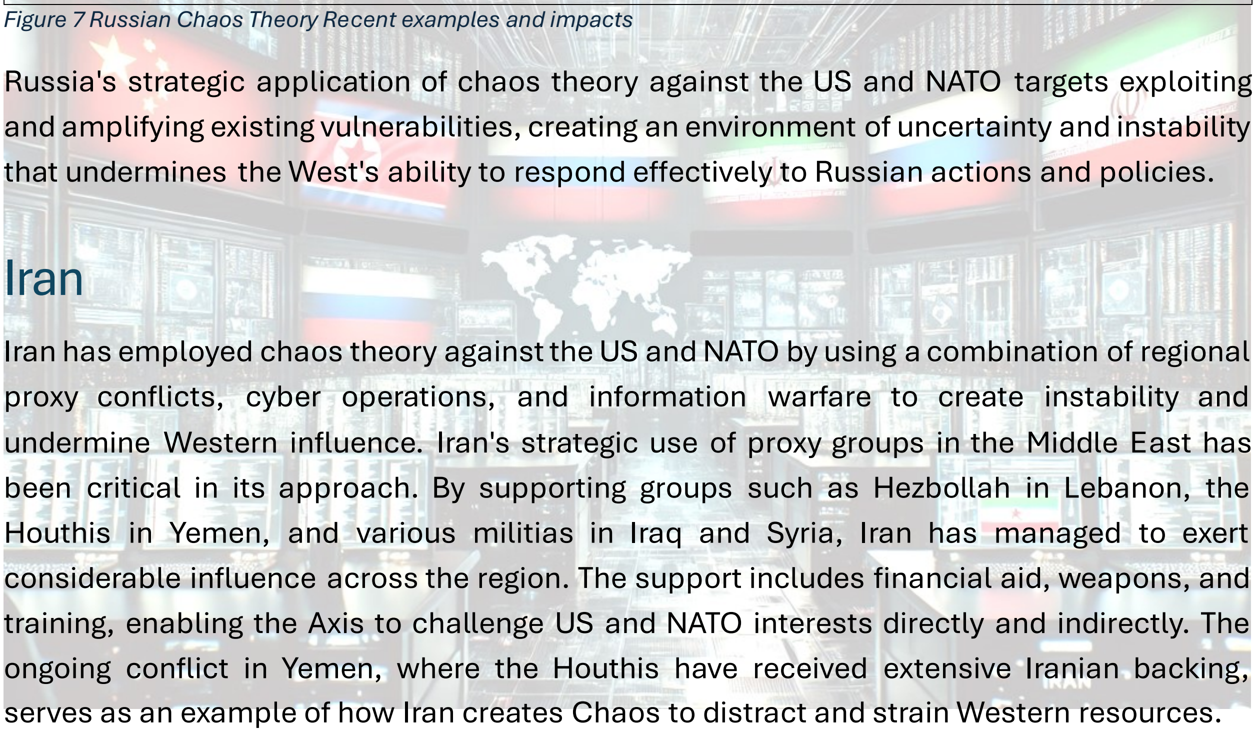
Furthermore, Russia's support for extremist groups and fringe political parties in Europe and the US has contributed to the destabilization of Western societies. By providing financial and ideological support to these groups, Russia amplifies radical voices that challenge mainstream political discourse and create an environment of Chaos and uncertainty.

Impact of Russia's Chaos Theory Strategies

Strategy	**Recent Example**	**Impact**
Disinformation campaigns	Interference in the 2016 US Presidential Election	Polarization, distrust in democratic processes
Cyber operations	NotPetya malware attack	Infrastructure disruption, economic damages

Strategy	Recent Example	Impact
Hybrid warfare	Annexation of Crimea	Confusion, plausible deniability, geopolitical instability
Economic manipulation	Control over natural gas supplies	Tensions within NATO, energy security concerns
Information warfare	Propaganda through RT and Sputnik	Undermined trust in government, exacerbated societal divisions
Support for extremist groups	Funding of fringe political parties in Europe and the US	Amplified radical voices, destabilization of political systems

Figure 7 Russian Chaos Theory Recent examples and impacts



Russia's strategic application of chaos theory against the US and NATO targets exploiting and amplifying existing vulnerabilities, creating an environment of uncertainty and instability that undermines the West's ability to respond effectively to Russian actions and policies.

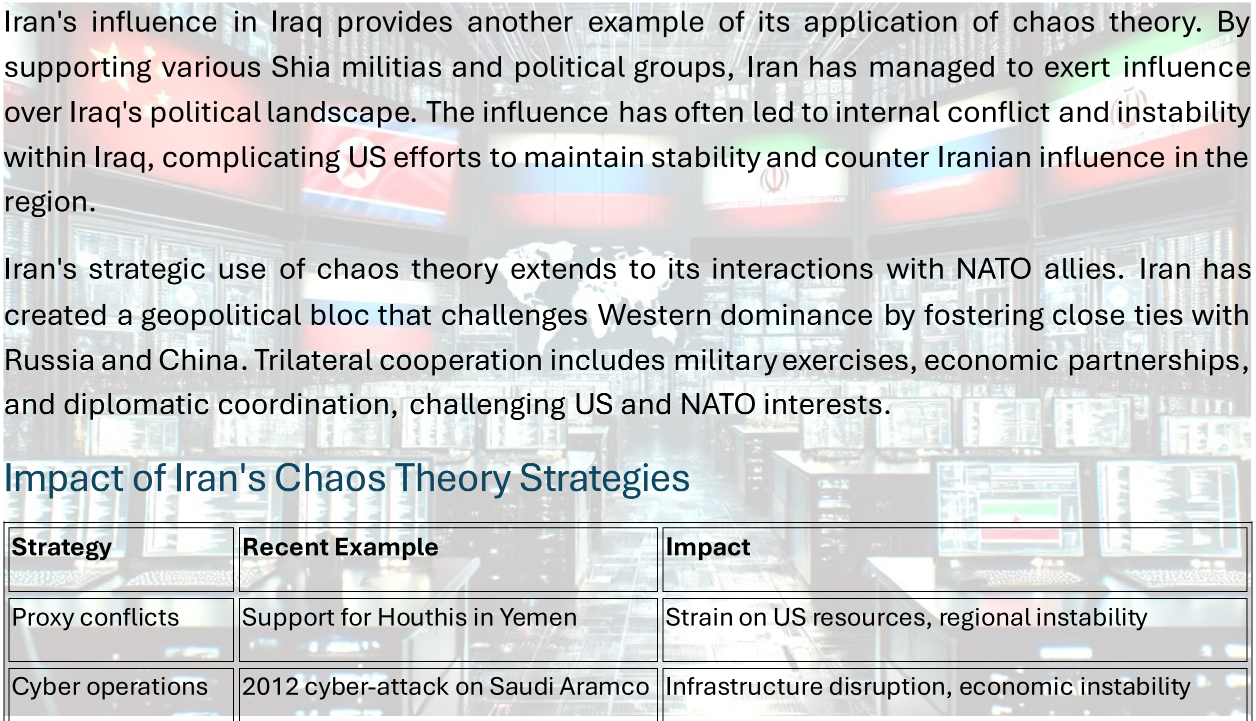
Iran

Iran has employed chaos theory against the US and NATO by using a combination of regional proxy conflicts, cyber operations, and information warfare to create instability and undermine Western influence. Iran's strategic use of proxy groups in the Middle East has been critical in its approach. By supporting groups such as Hezbollah in Lebanon, the Houthis in Yemen, and various militias in Iraq and Syria, Iran has managed to exert considerable influence across the region. The support includes financial aid, weapons, and training, enabling the Axis to challenge US and NATO interests directly and indirectly. The ongoing conflict in Yemen, where the Houthis have received extensive Iranian backing, serves as an example of how Iran creates Chaos to distract and strain Western resources.

Iran has also conducted cyber operations against US and NATO targets. One notable example is the 2012 cyber-attack on Saudi Aramco, attributed to Iranian hackers, which wiped data from thousands of computers and aimed to disrupt the operations of one of the world's largest oil producers. The attack demonstrated Iran's capability to inflict considerable damage on critical infrastructure. More recently, Iranian cyber actors have targeted US financial institutions, government agencies, and private companies, seeking to steal sensitive information, disrupt operations, and create economic instability.

Iran's information warfare strategy has focused on spreading disinformation and propaganda to influence public opinion and exacerbate existing societal tensions in the US and NATO countries. Iranian state media outlets, such as Press TV, have disseminated false narratives and conspiracy theories to undermine trust in Western governments and institutions. The efforts often align with broader geopolitical goals, such as discrediting US policies in the Middle East and portraying Iran as a victim of unjust Western aggression.

In addition to its cyber and information operations, Iran has employed economic tactics to create instability and exert pressure on the US and its allies. The strategic use of the Strait of Hormuz, through which much of the world's oil supply passes, allows Iran to threaten global energy security. Periodic threats to close the strait or disrupt shipping have created volatility in global oil markets, impacting Western economies and highlighting the vulnerabilities in global energy supplies.



Iran's influence in Iraq provides another example of its application of chaos theory. By supporting various Shia militias and political groups, Iran has managed to exert influence over Iraq's political landscape. The influence has often led to internal conflict and instability within Iraq, complicating US efforts to maintain stability and counter Iranian influence in the region.

Iran's strategic use of chaos theory extends to its interactions with NATO allies. Iran has created a geopolitical bloc that challenges Western dominance by fostering close ties with Russia and China. Trilateral cooperation includes military exercises, economic partnerships, and diplomatic coordination, challenging US and NATO interests.

Impact of Iran's Chaos Theory Strategies

Strategy	**Recent Example**	**Impact**
Proxy conflicts	Support for Houthis in Yemen	Strain on US resources, regional instability
Cyber operations	2012 cyber-attack on Saudi Aramco	Infrastructure disruption, economic instability
Information warfare	Disinformation through Press TV	Undermined trust in governments, exacerbated societal tensions
Economic tactics	Threats to close the Strait of Hormuz	Global oil market volatility, economic pressure on the West
Influence in Iraq	Support for Shia militias and political groups	Internal conflict complicated US stabilization efforts
Geopolitical alliances	Cooperation with Russia and China	Challenged Western dominance, ATTACK geopolitical threat

Figure 8 Iranian Chaos Theory Recent examples and impacts

Iran's application of chaos theory against the US and NATO involves exploiting regional conflicts, conducting cyber and information operations, and using economic tactics and geopolitical alliances to create instability and weaken Western influence. Their strategies target the exploitation and amplification of existing vulnerabilities, challenging the ability of the US and NATO to respond effectively.

North Korea

North Korea has effectively used chaos theory against the US and NATO by employing a blend of nuclear brinkmanship, cyber operations, information warfare, and geopolitical maneuvering to create uncertainty and instability. North Korea's nuclear program stands as the cornerstone of its strategy, creating significant geopolitical tension and forcing the US and its allies to engage in ongoing diplomatic and military preparedness. The regime's periodic missile tests, often conducted without warning, escalate regional tensions and provoke solid international responses. The tests not only demonstrate North Korea's growing capabilities but also serve to create a sense of unpredictability and Chaos.

Cyber operations are another critical component of North Korea's approach. The 2014 cyber-attack on Sony Pictures, attributed to North Korean hackers, highlighted the regime's ability to conduct high-profile attacks on foreign entities. The attack, which aimed to disrupt the release of a movie perceived as offensive to North Korean leadership, involved the theft and destruction of data and extensive media coverage, amplifying its impact. More recently, North Korean cyber actors have targeted financial institutions worldwide, engaging in cyber heists to fund the regime's activities and create economic disruption.

North Korea has also engaged in information warfare to shape perceptions and influence public opinion. The regime's state-controlled media, including outlets like KCNA, regularly disseminate propaganda designed to bolster domestic support and project an image of strength to international audiences. Additionally, North Korean operatives conduct disinformation campaigns to spread false narratives and create confusion among adversaries. They undermine the credibility of foreign governments and institutions, thereby sowing discord and uncertainty.

Geopolitical maneuvering by North Korea includes using its relationships with China and Russia to counterbalance US and NATO pressures. By maintaining close ties with other Axis states, North Korea gains strategic support and economic lifelines, which help mitigate the effects of international sanctions. The trilateral relationship complicates the geopolitical landscape, as any action against North Korea must consider the potential responses from China and Russia, adding layers of complexity and uncertainty to international diplomacy.

North Korea's exploitation of human rights abuses as a diplomatic tool also adds to its chaotic strategy. The regime often uses detained foreign nationals as bargaining chips, creating international incidents that force adversaries into delicate negotiations. The actions divert attention from broader strategic issues and create a climate of unpredictability and tension.

Impact of North Korea's Chaos Theory Strategies

Strategy	**Recent Example**	**Impact**
Nuclear brinkmanship	Periodic missile tests	Regional tension, diplomatic and military preparedness
Cyber operations	2014 cyber-attack on Sony Pictures	High-profile disruptions, economic impact
Information warfare	Propaganda through KCNA	Domestic support bolstered, international image of strength projected
Geopolitical maneuvering	Close ties with China and Russia	Strategic support, economic lifelines, diplomatic complexity
Human rights abuses	Detention of foreign nationals as bargaining chips	International incidents diverted strategic focus

Figure 9 North Korean Chaos Theory recent examples and impacts

North Korea's application of chaos theory against the US and NATO creates a multi-faceted challenge, blending military provocations, cyber-attacks, disinformation, and strategic alliances to exploit and amplify vulnerabilities in Western systems. The strategy effectively keeps adversaries off-balance and constantly engaged in addressing immediate crises, diverting resources and attention from broader strategic goals.

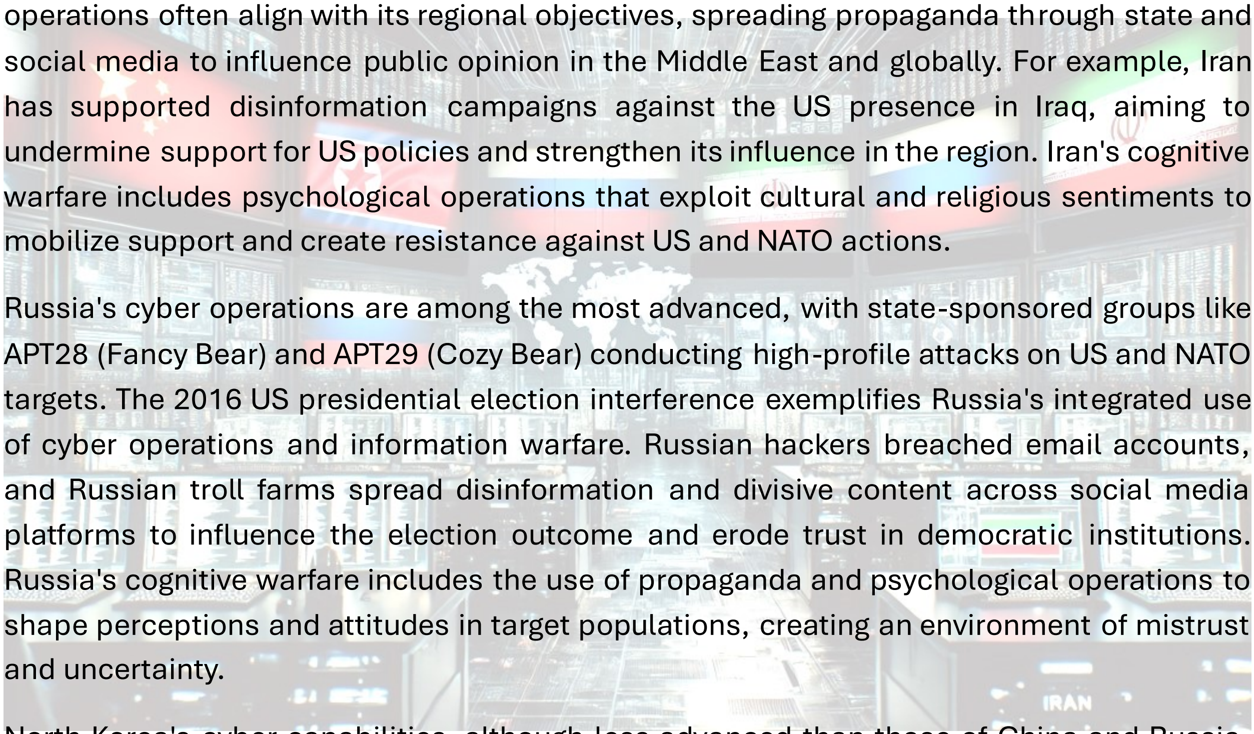
Operational Integration

China, Iran, Russia, and North Korea have the potential to integrate their cyber operations, information operations, and cognitive warfare against the US and NATO in a coordinated and systematic manner. Each country brings unique capabilities and strategic objectives, creating a formidable challenge for Western defenses.

China's extensive cyber capabilities include advanced persistent threat (APT) groups known for sophisticated cyber-espionage campaigns targeting US and NATO networks. For instance, APT10, linked to China's Ministry of State Security, has conducted extensive cyber espionage against Western governments, corporations, and military targets. China's information operations focus on spreading disinformation to manipulate public opinion and exacerbate societal divisions in Western countries. For example, during the COVID-19 pandemic, Chinese state media and social media accounts spread conspiracy theories about the virus's origins to deflect blame and sow confusion.

Iran has demonstrated its cyber capabilities through operations like the 2012 cyber-attack on Saudi Aramco and more recent attacks on US financial institutions. Iran's information operations often align with its regional objectives, spreading propaganda through state and social media to influence public opinion in the Middle East and globally. For example, Iran has supported disinformation campaigns against the US presence in Iraq, aiming to undermine support for US policies and strengthen its influence in the region. Iran's cognitive warfare includes psychological operations that exploit cultural and religious sentiments to mobilize support and create resistance against US and NATO actions.

Russia's cyber operations are among the most advanced, with state-sponsored groups like APT28 (Fancy Bear) and APT29 (Cozy Bear) conducting high-profile attacks on US and NATO targets. The 2016 US presidential election interference exemplifies Russia's integrated use of cyber operations and information warfare. Russian hackers breached email accounts, and Russian troll farms spread disinformation and divisive content across social media platforms to influence the election outcome and erode trust in democratic institutions. Russia's cognitive warfare includes the use of propaganda and psychological operations to shape perceptions and attitudes in target populations, creating an environment of mistrust and uncertainty.



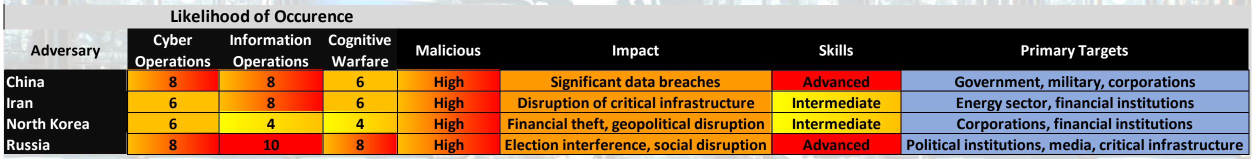
North Korea's cyber capabilities, although less advanced than those of China and Russia, have shown significant effectiveness in achieving strategic objectives. The 2014 Sony Pictures hack and cyber-attacks on global financial institutions demonstrate North Korea's willingness to use cyber operations to achieve geopolitical goals. North Korea's information operations include spreading propaganda to bolster the regime's image and influence perceptions internationally. The regime's cognitive warfare involves using fear and unpredictability to manipulate adversaries' actions and responses.

Comparative Analysis of Integrated Operations

Country	Cyber Operations	Information Operations	Cognitive Warfare
China	APT10 cyber-espionage campaigns targeting Western entities	Disinformation on COVID-19 origins	Psychological operations exploiting cultural sentiments
Iran	2012 cyber-attack on Saudi Aramco, attacks on US financial institutions	Propaganda through state media, anti-US disinformation in Iraq	Mobilizing support through religious and cultural narratives
Russia	2016 US election interference (APT28, APT29)	Social media disinformation campaigns	Propaganda to create mistrust and uncertainty
North Korea	2014 Sony Pictures hack, attacks on financial institutions	State propaganda to bolster regime image	Psychological operations using fear and unpredictability

Figure 10 Top 4 Integrated Operations

Levels of Maliciousness, Impact, Skill, and Targets



	Likelihood of Occurence						
Adversary	Cyber Operations	Information Operations	Cognitive Warfare	Malicious	Impact	Skills	Primary Targets
China	8	8	6	High	Significant data breaches	Advanced	Government, military, corporations
Iran	6	8	6	High	Disruption of critical infrastructure	Intermediate	Energy sector, financial institutions
North Korea	6	4	4	High	Financial theft, geopolitical disruption	Intermediate	Corporations, financial institutions
Russia	8	10	8	High	Election interference, social disruption	Advanced	Political institutions, media, critical infrastructure

Figure 11 Top 4 Scoring - Malicious, Impact, Skills, Targets

Integrating their operations, China, Iran, Russia, and North Korea coordinate cyber-attacks to create simultaneous disruptions across multiple sectors, overwhelming Western defenses. Concurrently, coordinated disinformation campaigns amplify societal divisions, creating confusion and weakening public trust in institutions. By sharing tactics, intelligence, and resources, the Axis enhanced the effectiveness of their cognitive warfare strategies, making it more difficult for the US and NATO to develop unified and effective responses.

For example, a coordinated cyber-attack on critical infrastructure by Russian and Iranian hackers, followed by disinformation campaigns from Chinese and North Korean operatives, creates a multi-ATTACK threat environment. The integrated approach exploits each country's strengths, using advanced cyber capabilities, strategic propaganda, and psychological operations to maximize disruption and achieve strategic objectives against the US and NATO.

Integrated Operations Example

Scenario	Impact	Response Challenges
Coordinated cyber-attack on power grids	Widespread blackouts, economic disruption	Overwhelmed cybersecurity defenses, delayed response
Simultaneous disinformation campaigns	Polarized public opinion eroded trust in institutions	Difficulty in countering false narratives, managing public perception
Psychological operations exploiting crises	Heightened fear and uncertainty, manipulated public behavior	Complex psychological impact, long-term societal effects

Figure 12 Integrated Ops Examples

The analysis underscores the potential for China, Iran, Russia, and North Korea to integrate their cyber operations, information operations, and cognitive warfare against the US and NATO, creating a complex and multi-dimensional threat environment that challenges Western capabilities and resilience.

Understanding Intelligence Risk in Cyber Operations, Information Operations, and Cognitive Warfare

We comprehensively understand Intelligence risk in cyber operations, information operations, and cognitive warfare by analyzing four key components: Probability of Threat, Probability of Success, Impact, and Target Vulnerabilities.

Probability of Threat (P(threat)) This metric assesses the likelihood that a specific Advanced Persistent Threat (APT) group will initiate a cyber attack. The evaluation considers the APT group's historical activity, frequency of attacks, and current operational levels. For instance, the threat probability is considered high if an APT group has a robust history of frequent and recent attacks.

Probability of Success of the Threat (P(success)) This factor evaluates the likelihood that an APT group's attempted attack will succeed. It considers the technical sophistication of the group, the historical success rate of its past attacks, and the defensive capabilities of potential targets. An APT group known for advanced technical capabilities and a high success rate in past attacks is more likely to succeed.

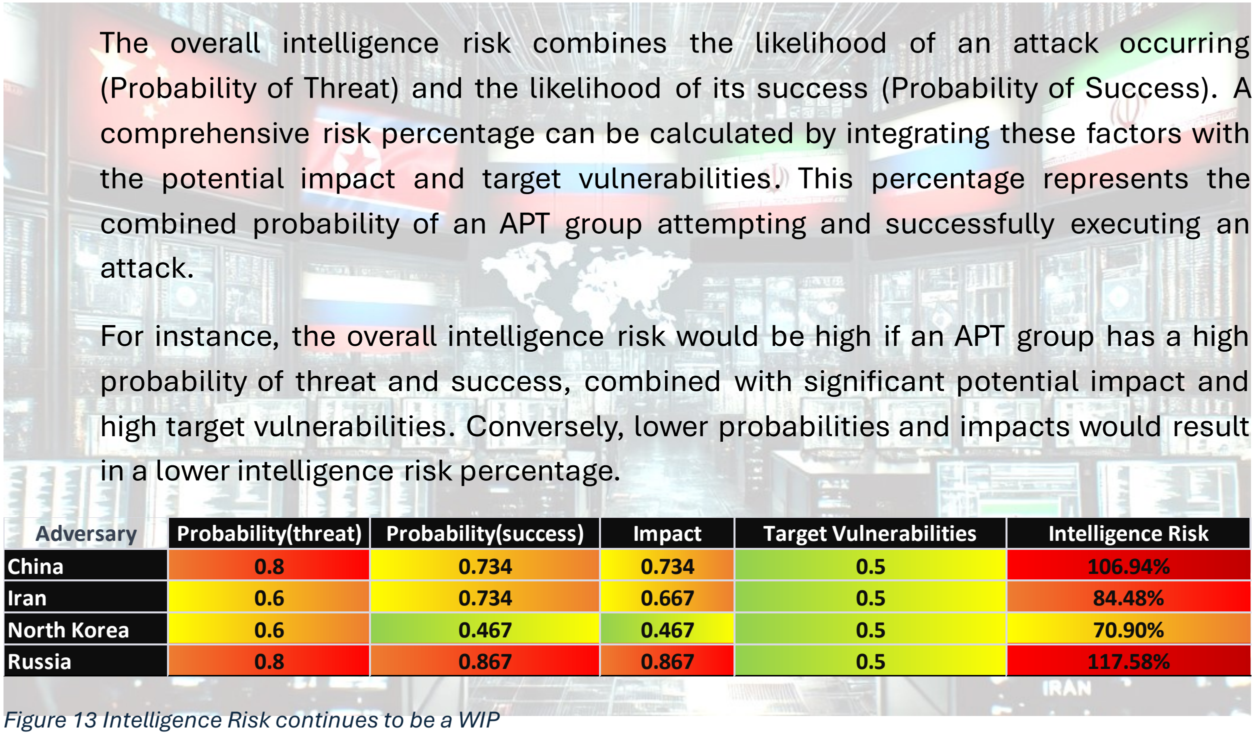
Impact Impact measures the potential consequences or severity of a successful attack by an APT group. This includes assessing the extent of potential data breaches, the value of stolen information, the disruption to critical services, and the broader implications for national security or economic stability. For example, an attack leading to significant data breaches and disruption of critical infrastructure would have a high impact.

Target Vulnerabilities This metric addresses the numeric vulnerability score of potential targets. Vulnerabilities can arise from weak cybersecurity practices, outdated systems, or the presence of high-value sensitive data. Due to the uncertainty of overall target vulnerabilities, a median score of 0.5 is assumed. This score helps gauge the susceptibility of potential targets to attacks.

Overall Intelligence Risk as a Percentage

The overall intelligence risk combines the likelihood of an attack occurring (Probability of Threat) and the likelihood of its success (Probability of Success). A comprehensive risk percentage can be calculated by integrating these factors with the potential impact and target vulnerabilities. This percentage represents the combined probability of an APT group attempting and successfully executing an attack.

For instance, the overall intelligence risk would be high if an APT group has a high probability of threat and success, combined with significant potential impact and high target vulnerabilities. Conversely, lower probabilities and impacts would result in a lower intelligence risk percentage.



Adversary	Probability(threat)	Probability(success)	Impact	Target Vulnerabilities	Intelligence Risk
China	0.8	0.734	0.734	0.5	106.94%
Iran	0.6	0.734	0.667	0.5	84.48%
North Korea	0.6	0.467	0.467	0.5	70.90%
Russia	0.8	0.867	0.867	0.5	117.58%

Figure 13 Intelligence Risk continues to be a WIP

Practical Application

Assessing intelligence risk using this framework allows for systematically evaluating potential threats. By understanding and quantifying each component, decision-makers can prioritize resources, enhance defensive measures, and mitigate potential risks effectively.

What is Next?

Expect significant developments from China, Iran, Russia, and North Korea, both individually and potentially in coordinated efforts, as they pursue their strategic objectives against the US and NATO.

China will continue to expand its cyber-espionage activities, targeting government, military, and corporate networks in the US and NATO countries. Anticipate further cyber-attacks aimed at stealing sensitive data and intellectual property, disrupting critical infrastructure, and conducting influence operations through disinformation campaigns. China's information warfare will likely focus on exacerbating existing social and political divides in Western societies, spreading false narratives and conspiracy theories to undermine public trust in democratic institutions. Cognitive warfare will exploit cultural and societal weaknesses, aiming to manipulate perceptions and behaviors through psychological operations.

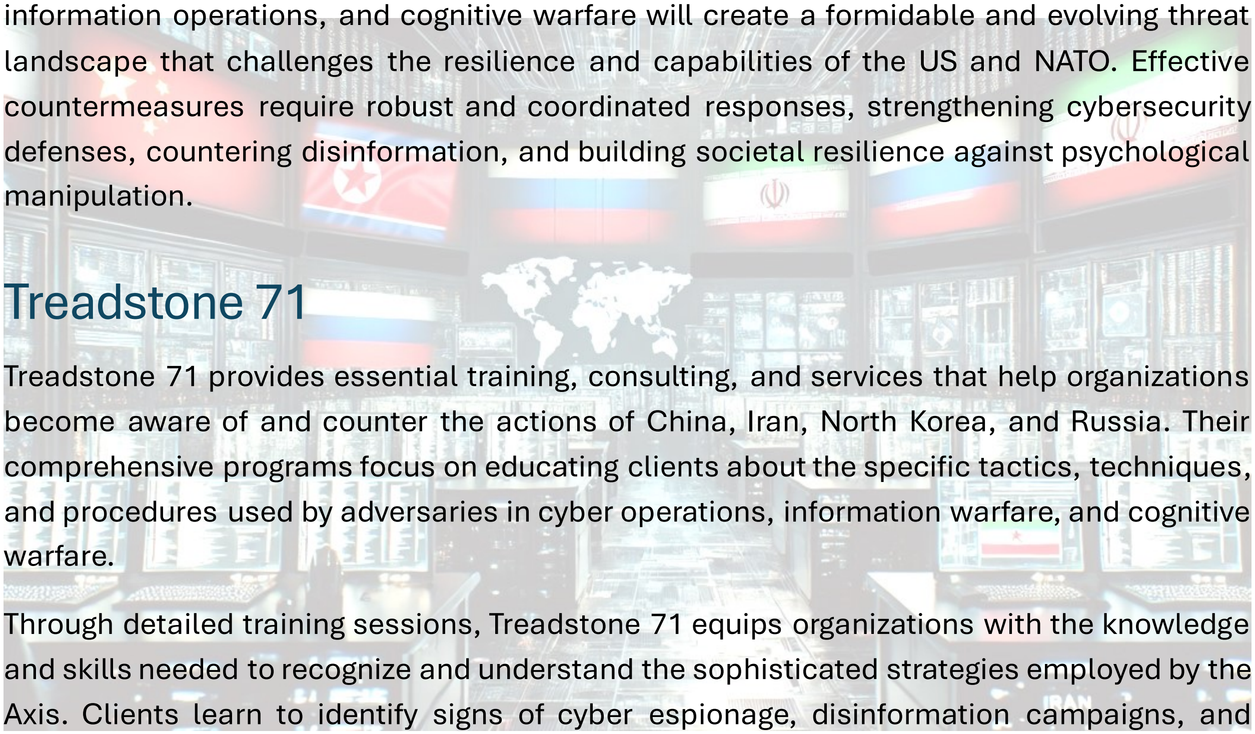
Iran's activities will likely intensify, with increased cyber-attacks on critical infrastructure in the US and NATO member states. Expect further attempts to disrupt financial systems, energy sectors, and government networks. Iran's information operations will continue to support its regional objectives, spreading anti-Western propaganda and disinformation through state media and social media channels. Iran will also use cognitive warfare to mobilize support within its regional sphere of influence, using cultural and religious narratives to counter US and NATO policies.

Russia will remain a significant threat, with sophisticated cyber operations targeting election systems, critical infrastructure, and media outlets. Anticipate further disinformation campaigns to polarize public opinion and undermine democratic processes in the US and NATO countries. Russia's cognitive warfare will focus on creating mistrust and uncertainty, using propaganda to shape perceptions and influence political outcomes. Russian efforts will also involve supporting extremist groups and fringe political movements to destabilize Western societies.

North Korea will continue its pattern of cyber-attacks on financial institutions and other high-value targets. Expect further efforts to steal funds and disrupt economic activities to support the regime's strategic objectives. North Korea's information operations will emphasize propaganda to bolster the regime's image and influence international perceptions. Cognitive warfare will involve creating fear and unpredictability and manipulating adversaries' actions and responses through psychological operations.

Potential coordinated efforts between adversary countries will present a complex and multi-dimensional threat environment. Combined cyber-attacks on critical infrastructure across the US and NATO countries create simultaneous disruptions, overwhelming defenses, and response capabilities. Joint disinformation campaigns amplify societal divisions and create confusion, weakening public trust in institutions. Coordinated psychological operations manipulate public behavior and exploit crises, further complicating response efforts.

Between now and December 31, 2024, anticipate the euphemistically identified "Axis of Evil" nations to refine and enhance their tactics, sharing intelligence and resources to maximize their impact. They will likely exploit geopolitical events, economic vulnerabilities, and social tensions to achieve their strategic objectives. The integration of cyber operations, information operations, and cognitive warfare will create a formidable and evolving threat landscape that challenges the resilience and capabilities of the US and NATO. Effective countermeasures require robust and coordinated responses, strengthening cybersecurity defenses, countering disinformation, and building societal resilience against psychological manipulation.



Treadstone 71

Treadstone 71 provides essential training, consulting, and services that help organizations become aware of and counter the actions of China, Iran, North Korea, and Russia. Their comprehensive programs focus on educating clients about the specific tactics, techniques, and procedures used by adversaries in cyber operations, information warfare, and cognitive warfare.

Through detailed training sessions, Treadstone 71 equips organizations with the knowledge and skills needed to recognize and understand the sophisticated strategies employed by the Axis. Clients learn to identify signs of cyber espionage, disinformation campaigns, and psychological operations. The awareness enables organizations to detect and respond to threats more effectively.

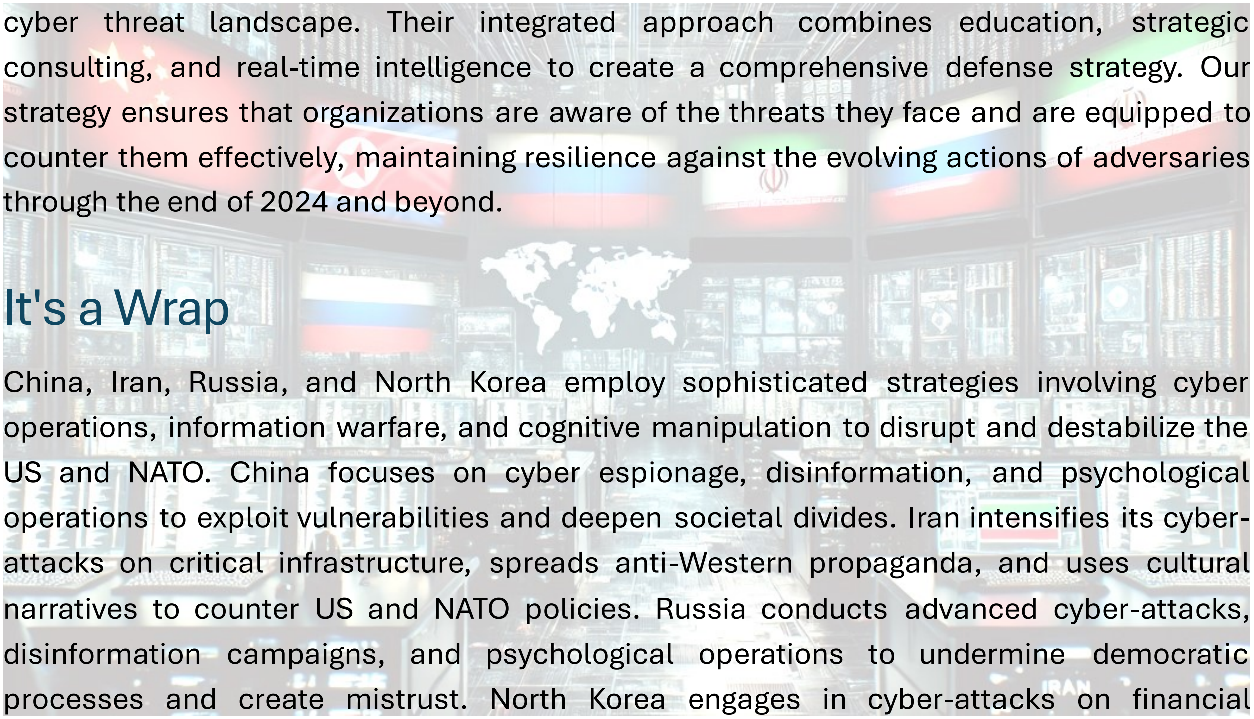
Treadstone 71's consulting services provide tailored advice and strategies to enhance an organization's defensive capabilities. They thoroughly assess existing security measures, identifying vulnerabilities that adversaries might exploit. Based on our assessments, they develop customized action plans to strengthen cybersecurity, improve information operations resilience, and counter cognitive warfare tactics.

The services offered by Treadstone 71 include ongoing threat monitoring and intelligence analysis. They continuously track the activities of China, Iran, North Korea, and Russia, providing clients with up-to-date information on emerging threats and potential attacks.

Real-time intelligence allows organizations to stay ahead of adversaries, anticipating their moves and preparing appropriate countermeasures.

Treadstone 71 helps organizations counter the actions of the Axis by implementing advanced cybersecurity practices, developing robust information security protocols, and enhancing overall threat detection capabilities. They offer specialized training in threat intelligence, enabling clients to collect, analyze, and act on intelligence related to their specific threats. The proactive approach helps organizations disrupt adversary activities before they cause significant harm.

Treadstone 71 empowers organizations to defend against the sophisticated tactics of China, Iran, North Korea, and Russia by fostering a deeper understanding of the geopolitical and cyber threat landscape. Their integrated approach combines education, strategic consulting, and real-time intelligence to create a comprehensive defense strategy. Our strategy ensures that organizations are aware of the threats they face and are equipped to counter them effectively, maintaining resilience against the evolving actions of adversaries through the end of 2024 and beyond.



It's a Wrap

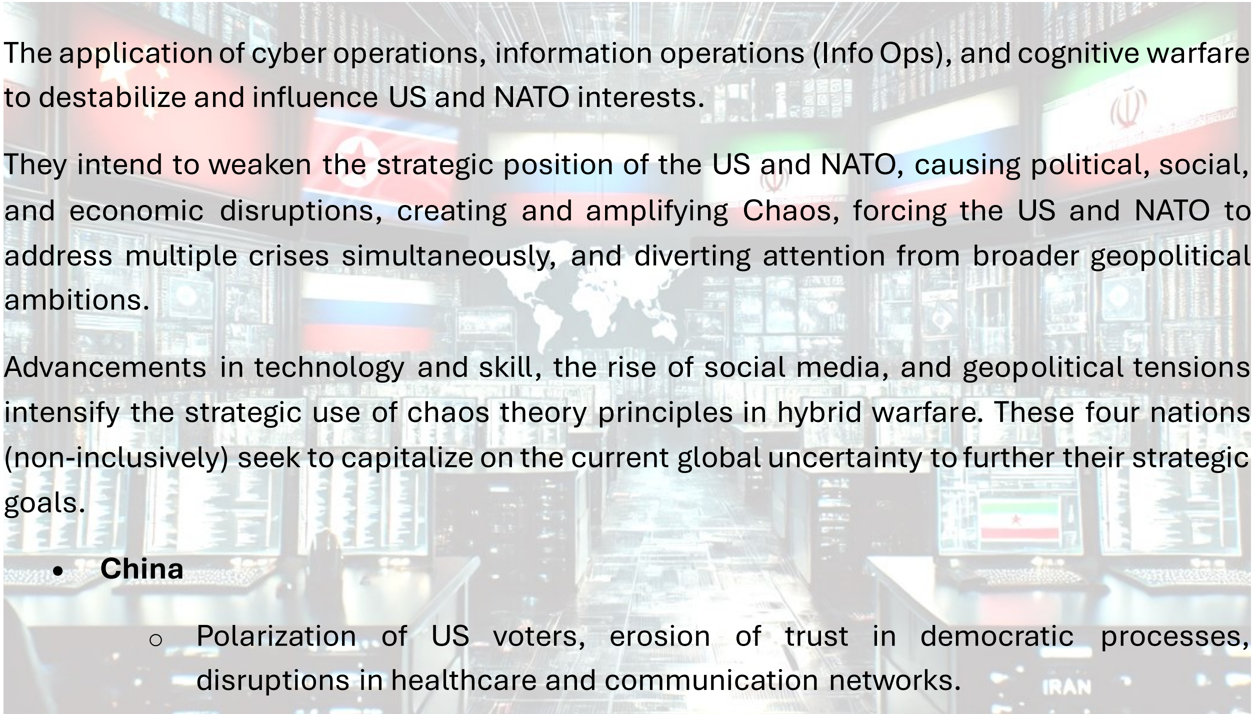
China, Iran, Russia, and North Korea employ sophisticated strategies involving cyber operations, information warfare, and cognitive manipulation to disrupt and destabilize the US and NATO. China focuses on cyber espionage, disinformation, and psychological operations to exploit vulnerabilities and deepen societal divides. Iran intensifies its cyber-attacks on critical infrastructure, spreads anti-Western propaganda, and uses cultural narratives to counter US and NATO policies. Russia conducts advanced cyber-attacks, disinformation campaigns, and psychological operations to undermine democratic processes and create mistrust. North Korea engages in cyber-attacks on financial institutions, spreads propaganda to bolster its regime, and uses psychological operations to manipulate adversaries. Their coordinated efforts present a complex and evolving threat landscape, challenging the resilience and response capabilities of the US and NATO.

Appendix A

Analytic Brief

Treadstone 71 assesses with high confidence that China, Iran, Russia, and North Korea will continue to use integrated and increasingly sophisticated cyber operations, information warfare, and cognitive manipulation strategies to disrupt and destabilize the US and NATO through 2024. Their coordinated efforts intend to exploit vulnerabilities in Western societies, creating an environment of uncertainty and instability that hampers effective response and resilience.

China, Iran, Russia, and North Korea



The application of cyber operations, information operations (Info Ops), and cognitive warfare to destabilize and influence US and NATO interests.

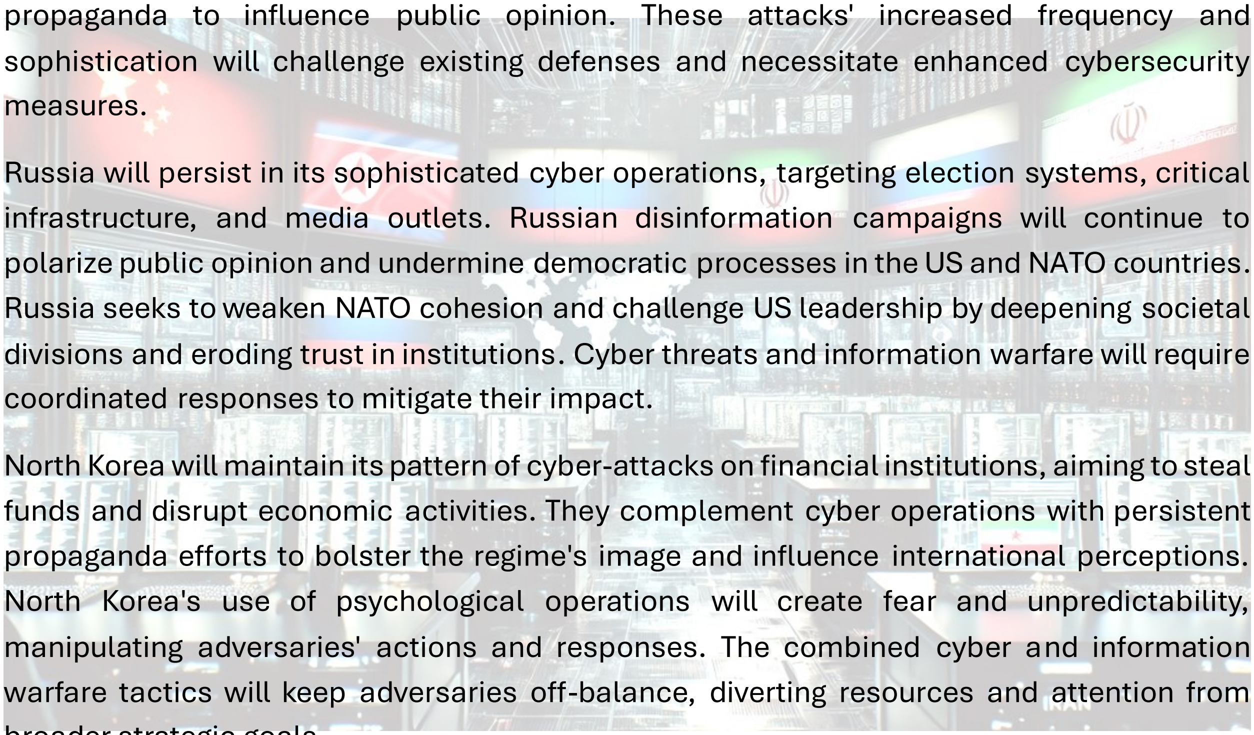
They intend to weaken the strategic position of the US and NATO, causing political, social, and economic disruptions, creating and amplifying Chaos, forcing the US and NATO to address multiple crises simultaneously, and diverting attention from broader geopolitical ambitions.

Advancements in technology and skill, the rise of social media, and geopolitical tensions intensify the strategic use of chaos theory principles in hybrid warfare. These four nations (non-inclusively) seek to capitalize on the current global uncertainty to further their strategic goals.

- **China**
  - Polarization of US voters, erosion of trust in democratic processes, disruptions in healthcare and communication networks.
- **Iran**
  - Intensified regional conflicts, strain on US resources, operational disruptions in the US.
- **Russia**
  - Weakened NATO cohesion, deepened political divides, and infrastructure disruptions.
- **North Korea**
  - Regional tension from nuclear tests, economic impacts from cyber-attacks.

China's expansion of cyber-espionage activities will likely target government, military, and corporate networks, seeking to steal sensitive data and intellectual property. Concurrently, China's influence operations will focus on exacerbating existing social and political divides in Western societies, spreading false narratives and conspiracy theories to undermine public trust in democratic institutions. The impact of these activities will strain resources and destabilize societal cohesion.

Iran's cyber-attacks on critical infrastructure will intensify, targeting financial systems, energy sectors, and government networks in the US and NATO member states. These attacks aim to disrupt operations and create economic instability, while Iran's disinformation campaigns will continue to support its regional objectives, spreading anti-Western propaganda to influence public opinion. These attacks' increased frequency and sophistication will challenge existing defenses and necessitate enhanced cybersecurity measures.



Russia will persist in its sophisticated cyber operations, targeting election systems, critical infrastructure, and media outlets. Russian disinformation campaigns will continue to polarize public opinion and undermine democratic processes in the US and NATO countries. Russia seeks to weaken NATO cohesion and challenge US leadership by deepening societal divisions and eroding trust in institutions. Cyber threats and information warfare will require coordinated responses to mitigate their impact.

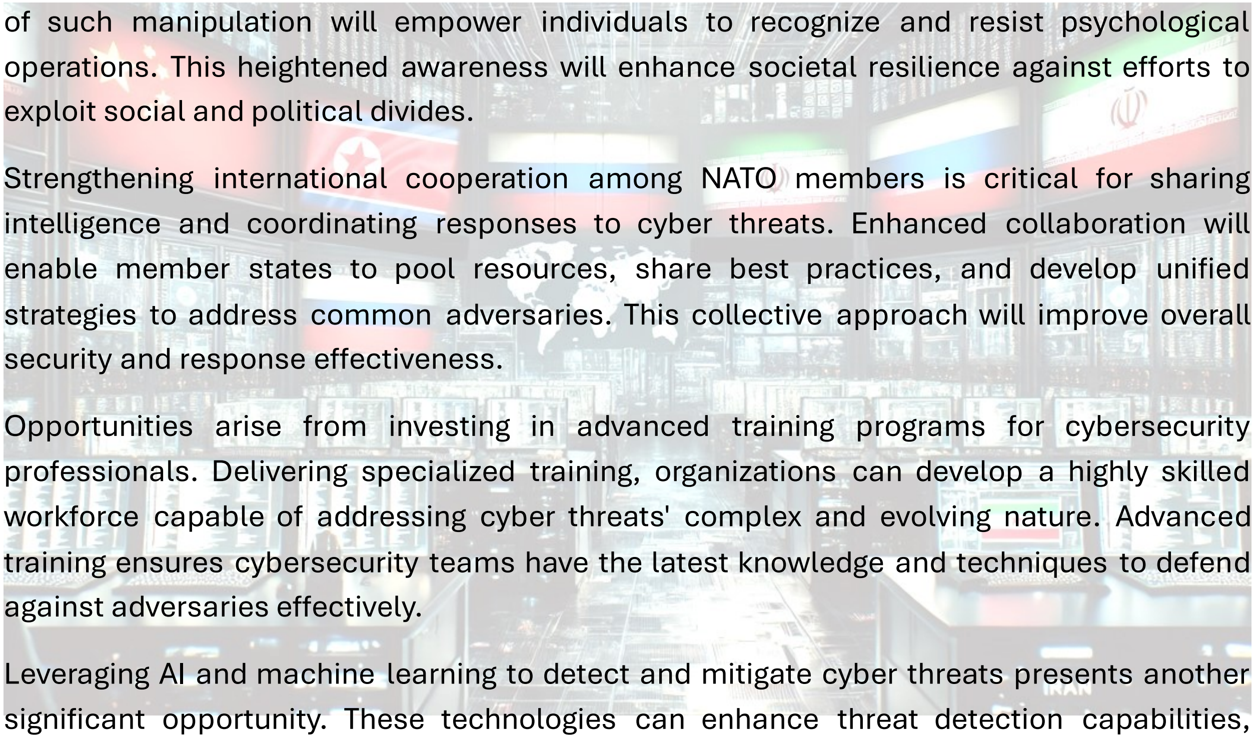
North Korea will maintain its pattern of cyber-attacks on financial institutions, aiming to steal funds and disrupt economic activities. They complement cyber operations with persistent propaganda efforts to bolster the regime's image and influence international perceptions. North Korea's use of psychological operations will create fear and unpredictability, manipulating adversaries' actions and responses. The combined cyber and information warfare tactics will keep adversaries off-balance, diverting resources and attention from broader strategic goals.

The potential for coordinated efforts of China, Iran, Russia, and North Korea creates a complex and evolving threat landscape, challenging the resilience and response capabilities of the US and NATO. Anticipating these developments, it is imperative to strengthen cybersecurity defenses, counter disinformation, and enhance public awareness to navigate and mitigate the impacts of these sophisticated tactics effectively.

Treadstone 71 recommends several strategic measures to counter the escalating cyber threats posed by China, Iran, Russia, and North Korea. First, it is essential to strengthen cyber defenses by enhancing cybersecurity measures across critical infrastructure sectors. The enhancements involve implementing advanced security protocols, conducting regular vulnerability assessments, and ensuring robust incident response capabilities. Improved cyber defenses will protect vital systems from increasingly sophisticated attacks and reduce the potential for operational disruptions.

To counter disinformation, developing and implementing robust information verification processes is crucial. These processes will help identify and mitigate the spread of false narratives and propaganda, maintaining the integrity of public discourse. By employing advanced verification tools and promoting media literacy, organizations can reduce the impact of disinformation campaigns and preserve public trust in democratic institutions.

Increasing public awareness about cognitive manipulation tactics is also a key recommendation. Educational initiatives to inform the public about the nature and methods of such manipulation will empower individuals to recognize and resist psychological operations. This heightened awareness will enhance societal resilience against efforts to exploit social and political divides.



Strengthening international cooperation among NATO members is critical for sharing intelligence and coordinating responses to cyber threats. Enhanced collaboration will enable member states to pool resources, share best practices, and develop unified strategies to address common adversaries. This collective approach will improve overall security and response effectiveness.

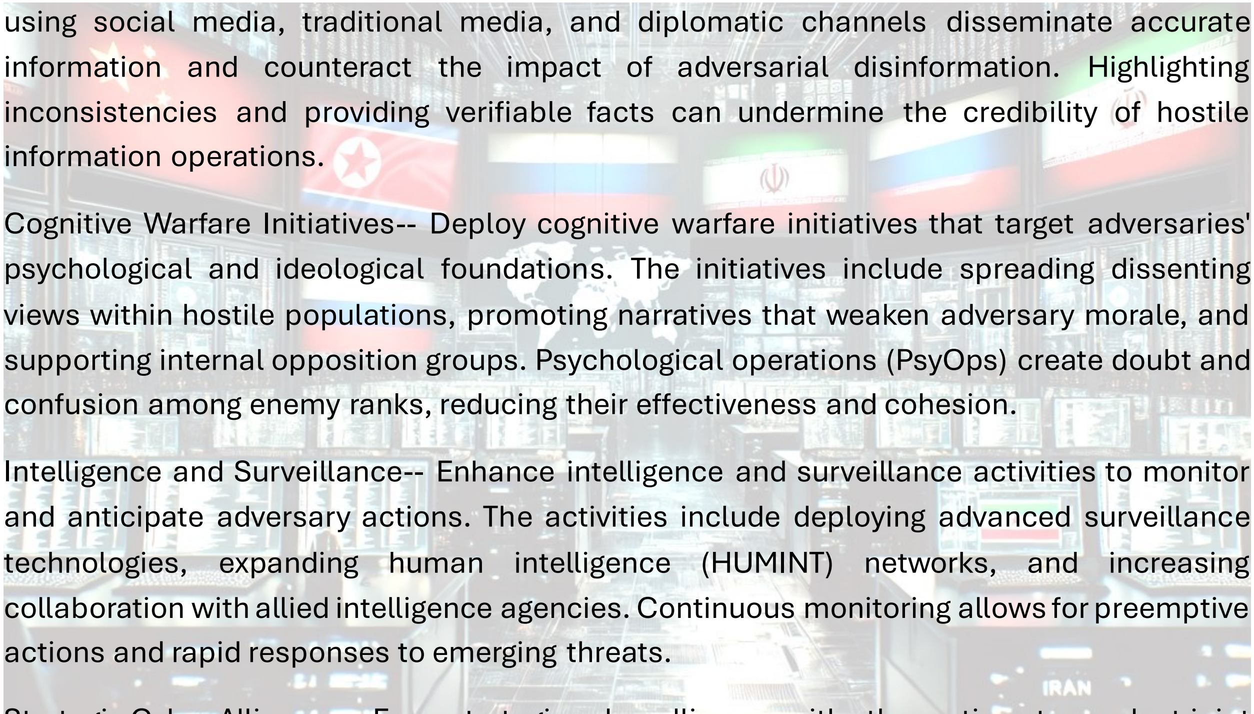
Opportunities arise from investing in advanced training programs for cybersecurity professionals. Delivering specialized training, organizations can develop a highly skilled workforce capable of addressing cyber threats' complex and evolving nature. Advanced training ensures cybersecurity teams have the latest knowledge and techniques to defend against adversaries effectively.

Leveraging AI and machine learning to detect and mitigate cyber threats presents another significant opportunity. These technologies can enhance threat detection capabilities, automate responses, and identify patterns that may indicate malicious activity. By integrating AI-driven solutions, organizations can improve their ability to anticipate and counter cyber-attacks.

Finally, strengthening strategic alliances with other nations facing similar threats will create a unified front against adversaries. Collaborative efforts can lead to the development of comprehensive defense strategies, shared intelligence, and coordinated actions that enhance global cybersecurity. Strategic alliances will provide a robust framework for addressing the challenges posed by state-sponsored cyber operations, information warfare, and cognitive manipulation.

Treadstone 71 recommends a series of counter and offensive actions to effectively respond to the cognitive warfare, cyber, and information operations employed by China, Iran, Russia, and North Korea. These proactive measures disrupt adversaries' operations, deter future attacks, and protect national security interests.

Cyber Countermeasures-- Implementing aggressive cyber countermeasures can disrupt adversaries' networks and operations, including deploying advanced cyber tools to identify and neutralize threats before they materialize. Offensive cyber operations deter by demonstrating the capability and willingness to respond in kind.



Active Disinformation Campaigns-- Develop and execute counter-disinformation campaigns to expose and discredit false narratives propagated by adversaries. Campaigns using social media, traditional media, and diplomatic channels disseminate accurate information and counteract the impact of adversarial disinformation. Highlighting inconsistencies and providing verifiable facts can undermine the credibility of hostile information operations.

Cognitive Warfare Initiatives-- Deploy cognitive warfare initiatives that target adversaries' psychological and ideological foundations. The initiatives include spreading dissenting views within hostile populations, promoting narratives that weaken adversary morale, and supporting internal opposition groups. Psychological operations (PsyOps) create doubt and confusion among enemy ranks, reducing their effectiveness and cohesion.

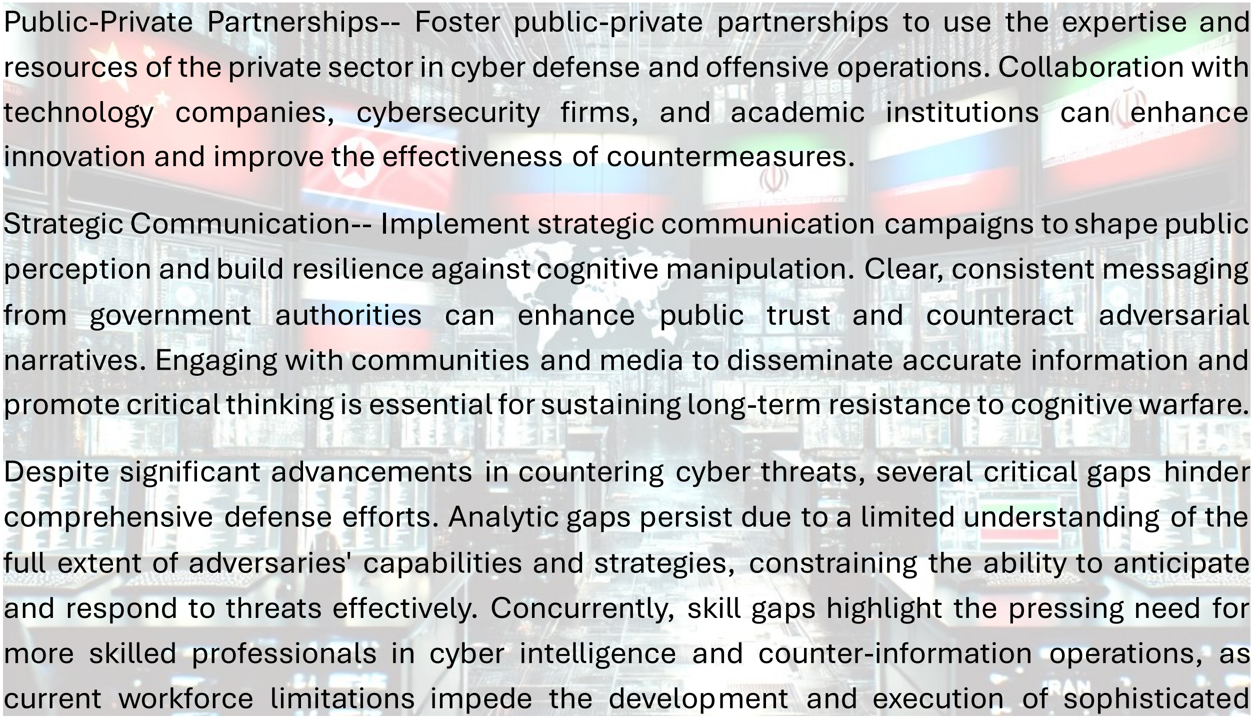
Intelligence and Surveillance-- Enhance intelligence and surveillance activities to monitor and anticipate adversary actions. The activities include deploying advanced surveillance technologies, expanding human intelligence (HUMINT) networks, and increasing collaboration with allied intelligence agencies. Continuous monitoring allows for preemptive actions and rapid responses to emerging threats.

Strategic Cyber Alliances-- Form strategic cyber alliances with other nations to conduct joint cyber operations and share intelligence. Collaborative efforts can amplify the impact of offensive actions and create a unified front against shared adversaries. These alliances can also facilitate coordinated responses to cyber incidents and improve overall resilience.

Offensive Information Operations-- Engage in offensive information operations to disrupt adversaries' communication channels and command structures. Such operations include hacking into and disabling propaganda websites, intercepting and manipulating communications, and deploying bots to flood adversary social media with conflicting information. Such actions can create operational confusion and hinder enemy coordination.

Technology Development and Deployment-- Invest in developing and deploying cutting-edge technologies to enhance offensive capabilities, such as artificial intelligence (AI) for automated threat detection, blockchain for secure communications, and quantum computing for advanced cryptographic solutions. These technologies can provide a strategic advantage in cyber and cognitive warfare domains.

Legal and Economic Actions-- Use legal and economic actions to counter adversaries' capabilities. Sanctions against individuals and organizations involved in cyber-attacks and information warfare can limit their resources and operational freedom. Additionally, legal measures to prosecute cybercriminals and hold states accountable for their actions can serve as a powerful deterrent.



Public-Private Partnerships-- Foster public-private partnerships to use the expertise and resources of the private sector in cyber defense and offensive operations. Collaboration with technology companies, cybersecurity firms, and academic institutions can enhance innovation and improve the effectiveness of countermeasures.

Strategic Communication-- Implement strategic communication campaigns to shape public perception and build resilience against cognitive manipulation. Clear, consistent messaging from government authorities can enhance public trust and counteract adversarial narratives. Engaging with communities and media to disseminate accurate information and promote critical thinking is essential for sustaining long-term resistance to cognitive warfare.

Despite significant advancements in countering cyber threats, several critical gaps hinder comprehensive defense efforts. Analytic gaps persist due to a limited understanding of the full extent of adversaries' capabilities and strategies, constraining the ability to anticipate and respond to threats effectively. Concurrently, skill gaps highlight the pressing need for more skilled professionals in cyber intelligence and counter-information operations, as current workforce limitations impede the development and execution of sophisticated countermeasures. Additionally, collection gaps, marked by incomplete data on the methods and effectiveness of adversary operations, further exacerbate these challenges, leaving vulnerabilities that adversaries can exploit. Addressing these gaps is imperative for enhancing national security and ensuring robust defenses against evolving threats.

China's Strategic Approach

China employs chaos theory to target social and political stability through sophisticated information operations and cyber warfare. Recent disinformation campaigns during US elections and cyber-attacks on critical infrastructure highlight China's strategy to polarize voters and create distrust in democratic institutions. The impact has been significant, causing disruptions and eroding public trust.

Russia's Strategic Approach

Russia uses a blend of disinformation campaigns, cyber operations, and geopolitical tactics to create uncertainty and destabilize Western societies. The 2016 US presidential election interference exemplifies Russia's integrated use of cyber operations and information warfare. The ongoing cyber-attacks on critical infrastructure and election systems aim to weaken NATO cohesion and undermine democratic processes.

Iran's Strategic Approach

Iran's use of regional proxy conflicts, cyber operations, and information warfare creates instability and undermines Western influence. By supporting militant groups and conducting cyber-attacks on US networks, Iran intensifies regional conflicts and creates economic instability. The strategic use of the Strait of Hormuz further exacerbates global energy security concerns.

Alternative Analysis

Adversaries may shift their focus to more covert operations, using advanced technologies like AI and quantum computing to enhance their cyber capabilities. They may also form new alliances to share intelligence and coordinate attacks, presenting a more complex and multi-dimensional threat environment.

The coordinated efforts of China, Iran, Russia, and North Korea pose a significant and evolving threat to the US and NATO. Addressing these threats requires a comprehensive approach that includes strengthening cyber defenses, countering disinformation, increasing public awareness, and fostering international cooperation. Treadstone 71 provides essential training and consulting services to help organizations build resilience against these sophisticated tactics.