RED5

REPORT

Human Decision-Making in Chaotic Environments:

Cognitive Resilience and Adaptive Strategy

CHIEF EDITOR Karna McGarry

FIRST LINE EDITOR Michael Searway

CONTRIBUTING AUTHORS Steven Duke, Dakota Hudson, Ethan Reeder, Isaac Chitwood, & Robert Gill

MESSAGE FROM THE CEO

In today's rapidly evolving threat environment, organizations are facing a level of complexity and volatility that challenges traditional approaches to security and risk analysis. From geopolitical instability and technological disruption to increasingly interconnected operational threats, the ability to adapt and make informed decisions in chaotic environments has never been more critical.

KRIS COLEMAN
FOUNDER & CEO, RED5

It is my privilege to introduce our latest white paper, ***Human Decision-Making in Chaotic Environments: Cognitive Resilience and Adaptive Strategy***. In this newest edition, our analysts examine how modern security teams can move beyond reactive, trend-driven approaches and adopt more adaptive, systems-based methods for identifying and mitigating emerging risks.

At Red5 Security, our commitment to helping clients anticipate and manage complex risks remains unwavering. By combining experienced human analysis with advanced technologies and adaptive analytical frameworks, we continue to strengthen our ability to provide actionable intelligence and proactive security solutions in an unpredictable world.

As the global environment continues to evolve, staying informed, agile, and resilient will remain essential. We hope this white paper provides valuable insight into the challenges ahead and the strategies organizations can adopt to better prepare for them.

TABLE OF CONTENTS

ABOUT RED5

ABOUT US

Red5 is a strategic intelligence and security consulting firm focused on identifying risk before it becomes disruption.

For more than 20 years, we have supported corporations, family offices, executives, and high-profile individuals with proactive intelligence, risk analysis, and advisory services designed to help clients make informed decisions in rapidly evolving environments.

Our approach combines rigorous intelligence methodology, human-led intelligence, experienced human judgment, and continuous assessment to identify early indicators others may overlook.

We do not simply respond to incidents. We help clients recognize, understand, and act on risk early enough to change the outcome.

WHAT WE DO

We partner with family offices, high-profile individuals, and corporations navigating increasingly complex threat environments.

Acting as trusted consultants, our approach combines rigorous intelligence methodology with experienced human judgment to continuously assess, advise, and protect—intervening before early signals escalate into consequence.

Red5 delivers discreet, responsive protection in an increasingly digital and interconnected world.
Preventing bad things from happening to good people is not a slogan. It is the reason we exist.

5 CORE TENETS

Confidentiality

Rigor

Authenticity

Agility

Responsiveness

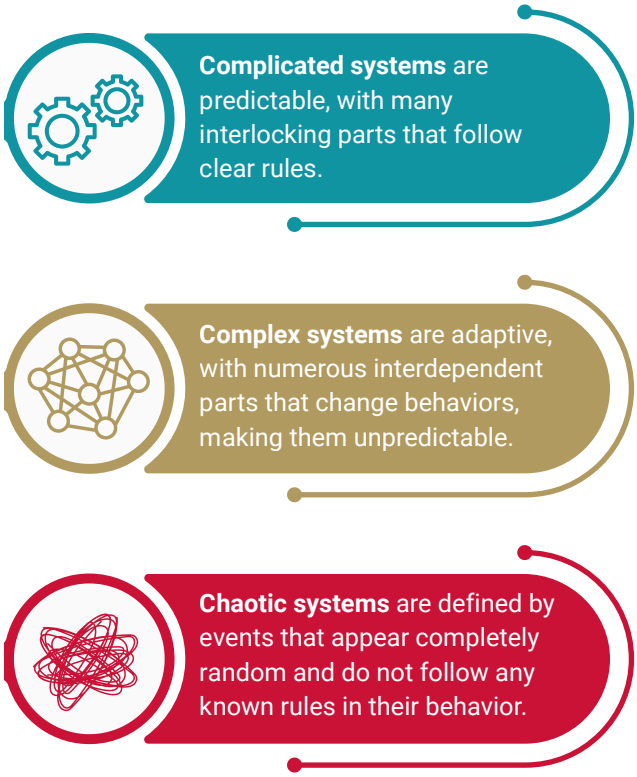
Introduction

Every year is shaped by its defining moments and emerging trends, and previous years have revealed how dangerous it is to be unprepared for rapidly evolving threats. Preparing for unknown variables can be challenging, and many security analysts and organizations fall victim to acting in a reactive approach.

Recent developments in the Middle East underscore how complex it is to assess situations involving multiple actors, as overlapping interests, shifting alliances, and asymmetric capabilities create rapidly changing conditions where a single event can trigger cascading political and economic consequences across regions.

In this increasing complexity of global events, traditional security analysis may not be sufficient and adopting a systematic thinking approach is crucial. This requires security and intelligence teams to move beyond reactionary and data-overwhelmed approaches by integrating human expertise with pattern recognition to proactively identify and mitigate emergent risks.

In chaotic environments, trying to predict "trends" can be challenging because shifting conditions may be unpredictable and hard to capture. Yet what appears chaotic in these fast-paced surroundings is a complex scenario that demands a deeper cognitive resilience and more adaptive decision-making.



Complicated, Complex, Chaos; to many these words are all synonymous when discussing a topic that isn't inherently clear. Yet their definitions have different meanings important to defining systems and their comprehensibility within systems theory.

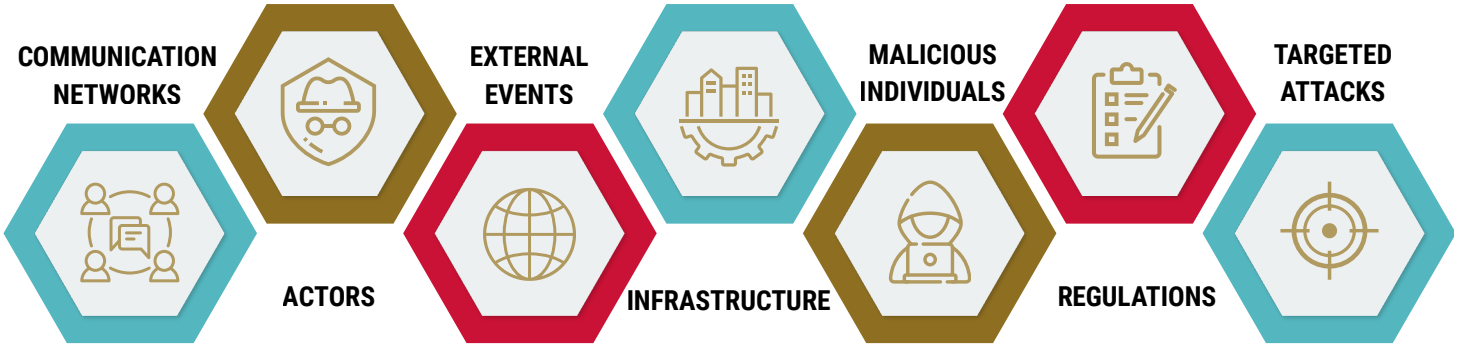
For additional information and definition see the works by Anticipatory Intelligence professional and National Intelligence University Professor Josh Kerbel.

Analytical Challenges in Nonlinear and Volatile Systems

Why Trends Are Outdated in a World of Chaotic Data

Historical trends can be beneficial when identifying potential patterns or vulnerabilities, but can construct siloed responses to security events. This creates a higher possibility that analysts are unable to sufficiently operate in the complex network of interconnected systems.

Threats often aren't isolated and to develop targeted mitigation strategies, security and intelligence teams must view threats as a network of:



Corporate Executive Officers, C-suite leaders, and board members have been plagued with major security risks in recent years, often characterized by chaotic environments. The overarching security environment created by these events begins to form 'trends.'

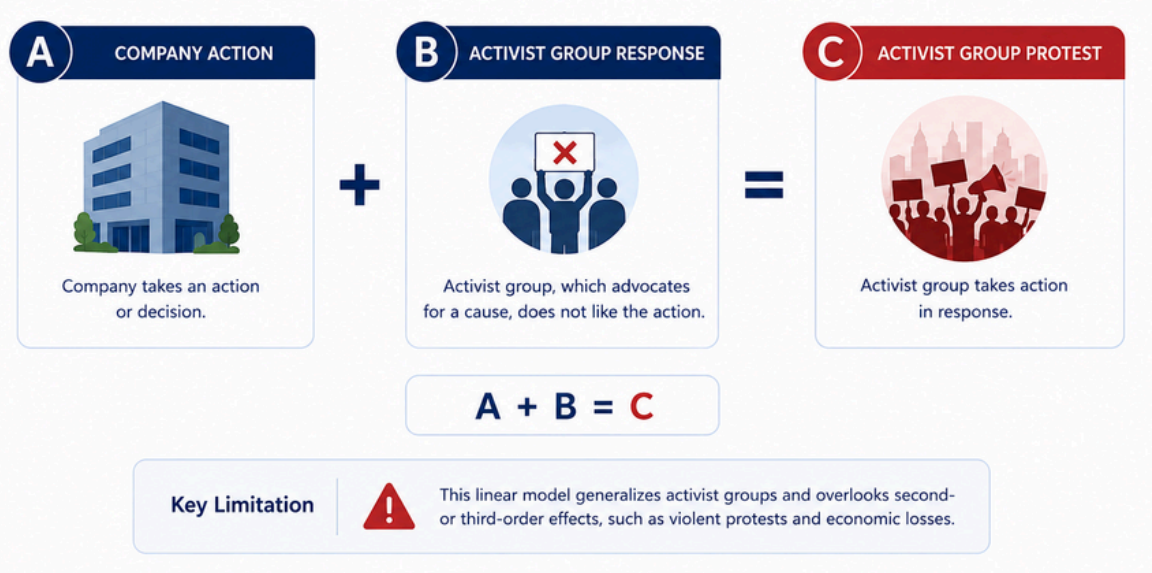
Hyper-focused events can create recency bias for analysts, leading to rigid thinking where nuance is lost and perceived influences are difficult to challenge.

This can silo analysts, causing them to overlook information that may connect events and, ultimately, preventing the development of a comprehensive analytical framework to effectively inform decision-makers.

Systems Thinking in Action

Systems thinking frames security as a network of interconnected events (“nodes”) rather than isolated incidents. Conventional analysis reduces risk to linear cause-and-effect, but this approach misses the broader interactions that shape outcomes.

A systems view enables security and intelligence professionals to identify how overlapping drivers and external pressures create second- and third-order effects, reducing blind spots and improving threat awareness.



In 2025, the U.S. saw over 10,000 activism events, highlighting activism's complexity. Understanding activism drivers is vital for identifying root causes and risks, as groups often overlap in issues.

For instance, a movement on inequality may intersect with anti-capitalism, pro-Palestinian, and environmental concerns, potentially spreading risks across sectors. This can lead to organizations, like pharmaceutical companies, facing scrutiny due to increased online rhetoric and legislative changes, even if they aren't directly involved.

After the assassination of UnitedHealthcare’s CEO, for example, focusing on C-suite or VIP assassinations became a trend in the security world. Security and threat analysts started to forgo searching for and noticing major security events unrelated to VIP and executive protection. In turn, other major events went largely unnoticed, unreported, and otherwise pushed aside.

One example was the lack of anticipation of mass disruption events, such as the SIM card event in New York City during the meeting of the UN General Assembly (UNGA).

A network of SIM cards and SIM servers were discovered by the Secret Service during the UNGA meeting in New York in late 2025, designed with the capability to send out mass electronic notices that could overwhelm and disrupt emergency networks during UNGA meetings.

While mass disruption of emergency services should not come as a surprise for security analysts, it did, despite the event being directly related to the 'trend' of VIP safety.

After the UnitedHealthcare assassination, in particular, physical security became the viewpoint from which analysts discovered events, and the silo of thinking and analysis was strong enough to prevent the security world from anticipating and exploring mass disruption at an event hosting many VIPs.


UN General Assembly | Patrick Gruban | Flickr

Chaos & Systems Thinking

Systems Thinking provides the framework for helping to identify and define the nodes of globally interconnected events, and allows the analysis of even more complex phenomena; i.e., concepts that appear to happen without direct causes.

Chaos theory suggests that while the world appears random, there are underlying cause-and-effect relationships that follow simple laws. The world viewed normally is chaotic; when viewed systematically, intelligence and security analysts can broaden their focus and recognize outcomes that may seem unpredictable.

While systems thinking helps map interconnected risks, it can become static if treated as a fixed model. By defining nodes and relationships at a single moment, analysts risk overlooking how quickly those dynamics can shift. Chaos theory addresses this gap by emphasizing that small changes can produce unpredictable, outsized effects. Together, they prevent analytical silos, ensuring security teams remain adaptive rather than constrained by rigid frameworks.

The very nature of chaos and emergent phenomena in complex environments leads to a higher volume of data that needs to be analyzed.

In a chaotic world, this can lead to the unconscious use of heuristics and bias encroachment to maintain efficiency, reducing thorough analysis of what is seemingly unrelated or irrelevant information.

What does this look like within intelligence and security teams? This is where decision fatigue, alert fatigue, and the feeling of “drinking from the firehose” emerges within teams, and this can be compounded by tools, such as artificial intelligence, that potentially repeat and exacerbate the underlying issue.

The Analytical Imperative to Break Information Silos

Analysts depend on the ability to understand the entire picture of a situation, yet information silos fragment that view into disconnected pieces, limiting accuracy and insight. When critical data is isolated across teams, systems, or formats, analysts are forced to make decisions based on incomplete or inconsistent information, introducing risk, inefficiency, and missed opportunities.

Breaking the “silo” of single event analysis is achieved through multiple tools and practices, including:

- AI-powered platforms working in conjunction with human input
- communication between analysts and decision makers
- the breakup of bureaucratic biases and strict adherence to subject matter expertise

Implementing these processes can mitigate information silos and allows analysts to realize the value of imaginative thinking and outside input.

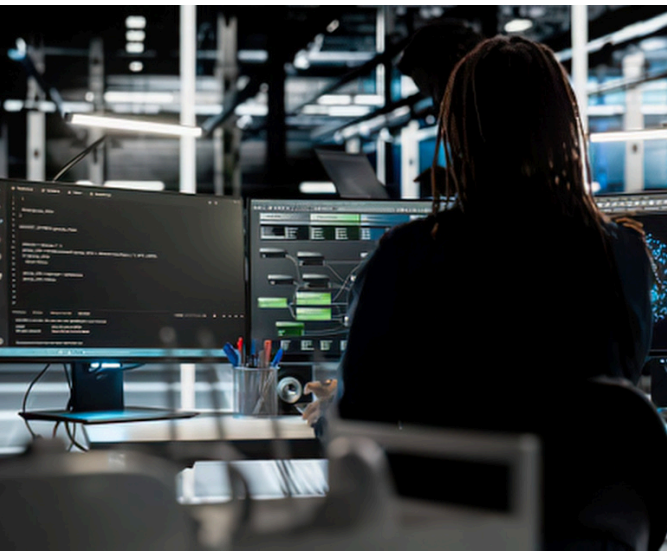
Collaboration is especially crucial for avoiding siloed analysis. Analysts cannot operate in a void; they must derive input from various stakeholders, such as marketing, government affairs, legal, and HR to create a comprehensive approach to address security risks.

Stakeholders outside of the traditional security analyst team can offer invaluable insight into emerging risks, and these insights operate as a segue to identifying alternative actors, or, in other terms, a gateway to break the typical reactionary cycle.

Breaking down these silos is not just a matter of convenience; it is essential for producing reliable analysis, uncovering meaningful patterns, and responding effectively to complex problems.

Shifting Security Postures in a Dynamic Threat Landscape

How Reactive Security Breaks Down Amid Complex, Interdependent Threats



Security professionals can thus become overwhelmed by chaos, falling victim to decision fatigue, pattern recognition biases, and historical trends resulting in mitigation strategies that fall short by only reacting to major events, not anticipating them.

To combat this, security and intelligence teams must proactively anticipate risks rather than rely solely on historical trends, which can be insufficient against adversaries rapidly adapting and exploiting emerging vulnerabilities.

Historical data still provides essential context, but paired with forward-looking strategies, such as innovative analytical frameworks and interdisciplinary collaboration, teams can move beyond reactive postures and develop more resilient, anticipatory security solutions.

In attempting to adapt in a world full of chaotic data, many have turned to new technologies, namely AI, which has seen increased use in the security field.

The use of AI has been notably helpful in scanning vast troves of data and identifying current trends that may have been missed by analysts utilizing traditional research methods.

However, most AI agents prioritize speed and task completion over security, often operating with overly permissive access that introduces vulnerabilities like prompt injection, model poisoning, and data exfiltration.

Additionally, the push to implement AI has often come at the cost of human expertise; many professionals in a variety of fields have quickly become overreliant on the technology while their own abilities have atrophied. These actions may be detrimental to future security decision making.

Analyst Input

Security analysts are seeing AI become more prevalent in the industry - both as a security risk that may cause breaches and manipulation, and as proficient tools that aim for speed and efficiency.

With such a polarizing advancement in technology, understanding a security analyst's thoughts on AI can provide critical insight for the future of the industry. Red5 Security surveyed security analysts who use machine learning tools to share their perspectives on this emerging technology in the industry and found that human oversight is still critical.

While AI's adaptive and cognitive capabilities are both impressive and advancing quickly, the role of human input continues to be fundamentally crucial, especially for security analysts. Utilizing AI as an efficiency tool alongside human feedback can help security teams provide proactive security approaches that combat seemingly chaotic risks.

At Red5 Security our specialized analysts and subject matter experts are empowered by industry-leading technology and our trusted process to assess, advise and protect our clients from current and emerging security concerns.

Moving Towards Adaptive Resilience in Complex Systems

The Human Element: Decision-Making in Chaotic Environments

While AI supports a more interconnected, systems-based approach, analysts remain essential for interpreting nuanced relationships and delivering informed, holistic assessments to decision-makers.

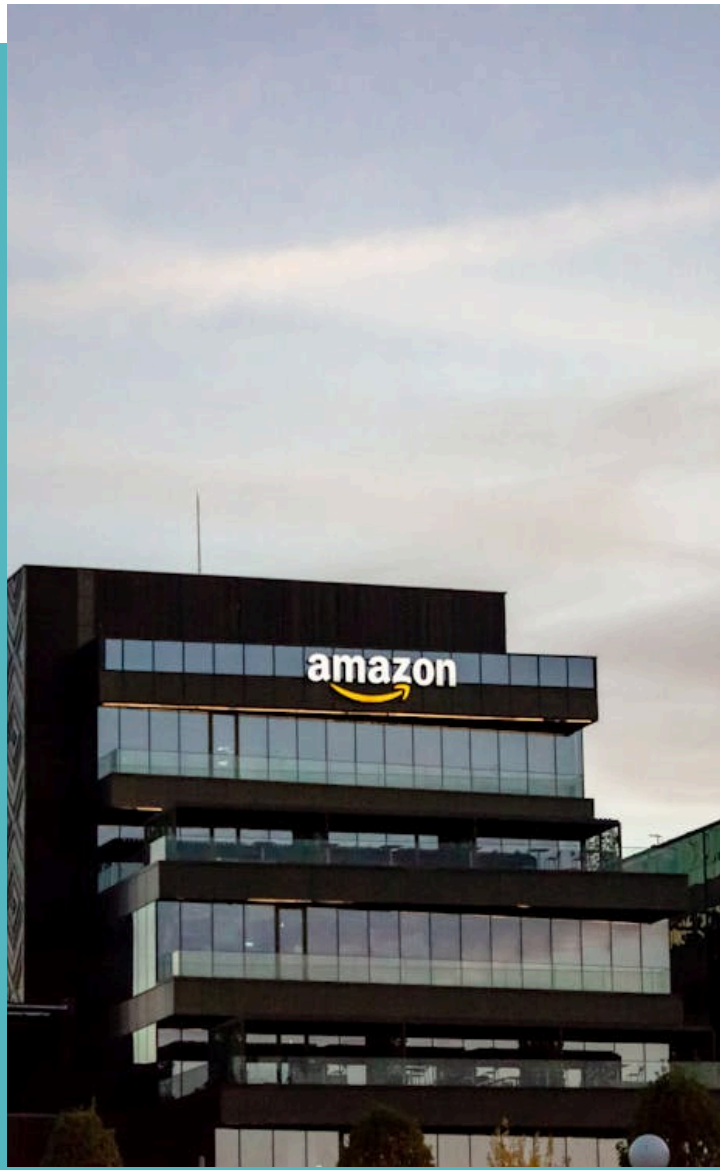
Uncovering seemingly chaotic elements and identifying relationships between them can transform how analysis is conducted.

A current example is the impact on global technology companies and the vulnerability of data centers in regions that are seeing kinetic conflicts.

Multiple data centers belonging to Amazon Web Services (AWS) were struck by Iranian missiles in Bahrain and the UAE in March.

Iranian media stated that the targeting of data centers was deliberate due to AWS supporting military and intelligence activities.

While the use of enterprise cloud computing for military operations has been an increasing trend, looking at this situation using systems thinking is also critical for private corporations, as these strikes had disruptive consequences across banking, delivery apps, enterprise software, and other areas.



Using chaos theory and systems thinking can anticipate potential similar disturbances; a conflict that is initially limited to nation-state military operations can escalate and impact commercial enterprises and daily operations, leading to increased risk to:

REPUTATION **SYSTEMS** **PERSONNEL** **FACILITIES**

Thinking from a systems perspective can mitigate the impacts of emergent phenomena and build resilience in any given industry.

Decision makers and executives, informed by more open analytical environments and teams using this systems thinking, can encourage cooperation with counterparts in different industries (systems) to better anticipate challenges that might pose future risks.

In chaos, understanding the relationship between what might, at first, seem unrelated, can help create analytical teams and environments that allow for more efficient operations and assessments that makes resilience build on itself via feedback loops.

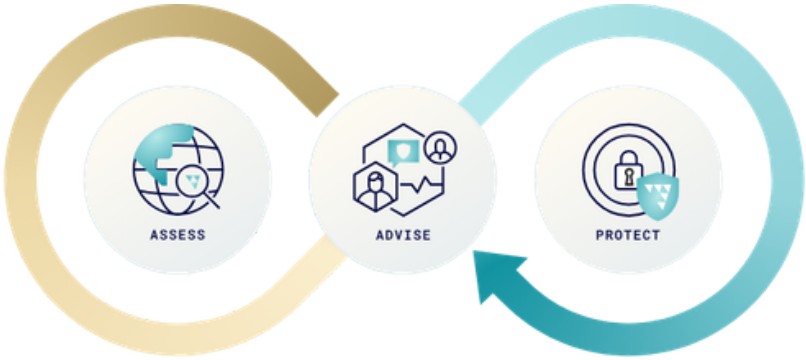
How Red5 Can Help Navigate Complex Threat Environments

The current threat landscape is unpredictable, with risks like geopolitical instability, activism, and cyber threats evolving rapidly. Traditional reactive security methods are insufficient for modern risk management.

Red5 Security assists organizations in transitioning to proactive, intelligence-driven security strategies. By leveraging experienced analysts and advanced technology, they provide actionable intelligence to help clients anticipate and mitigate risks before they escalate.

CONTINUOUS INTELLIGENCE

Red5 delivers continuous intelligence monitoring and analysis tailored to each client's operational environment, industry, and risk profile. Our analysts assess how emerging threats, online rhetoric, geopolitical developments, activism, and operational disruptions intersect to create broader security risks.



CONSULTING SERVICES

Red5 offers consulting services alongside intelligence support to enhance organizational resilience and decision-making during complex security events. Our expert team collaborates with clients to provide tailored solutions that align with operational priorities, security concerns, and business objectives.

GET IN TOUCH TO LEARN MORE

red5security.com/contact-us

info@red5security.com