Uncovering drivers of cyber behavior

A white paper on precision communication analysis

Introduction

This paper describes precision communications analysis capabilities that can be leveraged to support full-spectrum mission activities across a broad range of state and non-state cyber actors, each of which pose a significant and growing threat to U.S. national and economic security interests.

Precision analysis of communications, events, and attributable behaviors reveals actionable insights into the drivers of a cyber actor's behavior—their connections, motivations, wants, fears, and goals, as well as their overarching strategies and intent.

Precision communications analysis provides comprehensive intelligence based on data-driven evidence to support the ability to gain improved situational awareness and to anticipate changes in the cyber warfare environment, including meaningful changes in an adversary's strategy, and how future conditions may alter an adversary's trajectory.

Further, the outcome from precision communications analysis directly supports strategy and mission objectives to deter and dissuade unwanted cyber behavior. These outcomes are achieved through precision analysis that identifies what is aligned with strategy and norms of behavior and what may be a deviation from established patterns of norm. Analytic precision provides the ability to distinguish between the motivations and strategies of cyber actors using various tactics: cyber espionage, cyber theft and/or potentially disruptive cyberwarfare attacks.

What is precision communication analysis?

Perspecta's precision communications analysis capability to provide actionable insights into a wide range of cyber actors based on comprehensive analysis of actual communication(s) from individuals or cyber groups. A communication can be in any form, and from any available source (e.g. written statements, speeches, articles, e-mails, etc.). Communications are analyzed in context with shaping events, known behaviors and relevant secondary research.

Perspecta applies a scientifically validated approach through a proven, evidence-based analytical methodology to deliver a comprehensive understanding of a cyber actor or potential cyber adversary (whether a nation-state or non-state group). Analytical results reveal detailed insights to support plans and operations:

- How cyber actors view their world, their relationships and behavioral norms
- Key cyber actor decision-makers
- Decision-making processes
- Potentially uncover cyber actors' intent and goals

Precision Communications Analysis techniques can also be used to establish measures of effectiveness and key performance indicators that can track and measure changes and mission impact over time.

A wide range of analytic services and deliverables can be provided, many of which are inter-related, such as strategic and operational landscape analysis, competitive communication analysis, worldview and decision-making analysis, leadership and authorship profiles, and quick-look reports.

Strategic and operational landscape analysis

Plans and operations (and exercises) can be supported and sustained through Strategic and Operational Landscape Analysis that correlates cyber events with key cyber actor communications over time. Our approach objectively and systematically analyzes communications, behaviors, and contextual events using qualitative and quantitative techniques to identify patterns and trends. Mission abilities are enhanced as patterns and trends help identify cyber threat vectors – before, during and after cyber attacks – and anticipate future outcomes. Capturing and analyzing past relevant data significantly improves an evidence-based means to establish norms of behavior and early indicators of deviation from the norm.

- Is the adversary engaged in coordinated activities with other non-US allies?
- What is the nature of the coordination, and are there vulnerabilities that can be exploited?
- What early indicators (indications and warning) may exist that a change in strategy or tactics is coming?
- How can the adversary be expected to react to specific operational scenarios that they may occur in the future? (Mission Forecasting, Scenario and Risk-Based Planning)

Competitive communication analysis

To fully understand how others view U.S. actions and cyber defense postures, Perspecta provides Competitive Communication Analysis of communications statements, speeches, journals, strategy documents, Social Media, Blogs, etc., from likely adversary leaders and influencers on their views related to relevant issues, such as cyber warfare, electronic espionage, exfiltration, IP theft and Internet Governance.

Worldview and decision-making analysis

The formulation, sustainment and execution of plans and operations can be significantly enhanced through comprehensive analysis of cyber actors (nation states, groups and individuals). Worldview and decision-making analysis can reveal evidence-based insights such as:

- Who are the adversary's main messengers and decision-makers on key issues of interest?
- What are their objectives, beliefs, perceived sources of strength and perceived fears?
- What is their human social network of influencers, and who has influence over them?
- What is the adversary's true strategic direction, and what role do their operational cyber tactics play to help them achieve their strategy?

Leadership and authorship profiles

Leadership Profiles can be developed on specific identified central cyber decision makers that could adversely affect U.S. interests. Resulting knowledge gained from analysis could provide decision-makers with actionable insights and enable leaders to influence actions to change the behavior of the cyber actor.

- How can their behavior be modified?
- What strategy options would likely succeed with a high degree of confidence?
- What key performance indicators can be used to measure effectiveness to track and measure moderated leadership behaviors over time?

Perspecta's validated methodology produces, with precise accuracy, authorship profiles of individual communiques—even if they are delivered/posted online anonymously, or under a multitude of user IDs or pseudonyms. This capability may be applied to address a range of challenges (related to the tracking of specific leaders or other non-state actors) to discern the source of online content and messaging activity.

Quick-look reports

For specific communications of operational interest, Quick-Look Reports can be provided for rapid assessment of specific communication(s). Quick-Look reports can be used to provide a mission-impacting and timely assessment of any major shift in strategy or intent—useful in support of plans and operations. Once a knowledge baseline is established, rapid analysis provides an assessment of how a new development compares to established patterns and trends of behavior.

Summary

Precision Communications Analysis capabilities can be used in support of a full-spectrum mission approach to cyber operations. The capabilities range and can be adapted or combined in various configurations to address a multitude of challenges. At the core of the capability is the recognition that cybersecurity is not merely a technical problem. The critical actors making decisions on matters of cyberwarfare are people—whose communications and behaviors may be analyzed to reveal critical insights necessary for illuminating the drivers of problematic behavior and using that to dis-incentivize, deter, and accurately anticipate what may be coming next.

Because cybersecurity is not merely a technical problem, finding greater peace and stability in cyberspace will require more than a technical solution. Technical capabilities may be complemented by deep insights on the context, situation, motivations, and influences on human decision-makers. Only when such capabilities are combined, is full defense and deterrence possible.

Learn more at perspecta.com

perspecta™

perspecta.com | contactus@perspecta.com
15052 Conference Center Drive
Chantilly, Virginia 20151