# Predictive Analysis of Adversarial Cyber Behavior

## (STO-TR-IST-129)

# Executive Summary

This report summarizes the work and findings of the North Atlantic Treaty Organization (NATO) Research Task Group (RTG), IST-129, on Predictive Analysis of Adversarial Cyber Operations. The work of this RTG was initiated in late 2015 and completed in April 2019. The RTG Chair was Dr. Dennis McCallam, Northrop Grumman Corporation, United States.

The work of the RTG represents one of the initial, if not the initial, attempt at organizing at an international level the evaluation of prior research into predicting cyber events. The RTG found overall there was little in the way of direct research and solutions of predicting a cyber-adversary who launches an attack against a known vulnerability with an unknown exploit. As such, the work of IST-129 contains a body of work that will provide researchers and organizations a point of departure for continuing research.

# Analyse prédictive du cybercomportement des adversaires

## (STO-TR-IST-129)

# Synthèse

Le présent rapport résume les travaux et résultats du groupe de recherche (RTG) IST-129 de l'Organisation du Traité de l'Atlantique Nord (OTAN) sur l'analyse prédictive du cybercomportement des adversaires. Les travaux du présent RTG ont été lancés fin 2015 et achevés en avril 2019. Le Dr Dennis McCallam, de Northrop Grumman Corporation, États-Unis, a assuré la présidence du groupe de travail.

Les travaux du RTG constituent l'une des tentatives initiales, si ce n'est la première, d'organiser au niveau international l'évaluation des recherches antérieures portant sur la prédiction de cyberévènements. Le RTG a découvert qu'il existait peu de recherches directes et de solutions pour prédire les attaques d'un cyberadversaire contre une vulnérabilité connue, mais sous une forme encore inconnue. À ce titre, les travaux de l'IST-129 constituent un corpus qui fournira aux chercheurs et organisations un point de départ pour poursuivre les recherches.