START
NATIONAL CONSORTIUM FOR THE
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

RESEARCH BRIEF

Insider Threat for Inbound International Air Cargo

OVERVIEW

The *Insider Threat for Inbound International Air Cargo Project* arose out of an identified requirement from the Department of Homeland Security for an assessment of insider risks with respect to international air cargo bound for the United States from last points of departure abroad. The threat focus was radiological and nuclear (RN) terrorism, ranging from use of a cargo aircraft's payload to deliver improvised nuclear devices into U.S. airspace, to attempts to smuggle special nuclear materials or other radiological substances into the U.S.

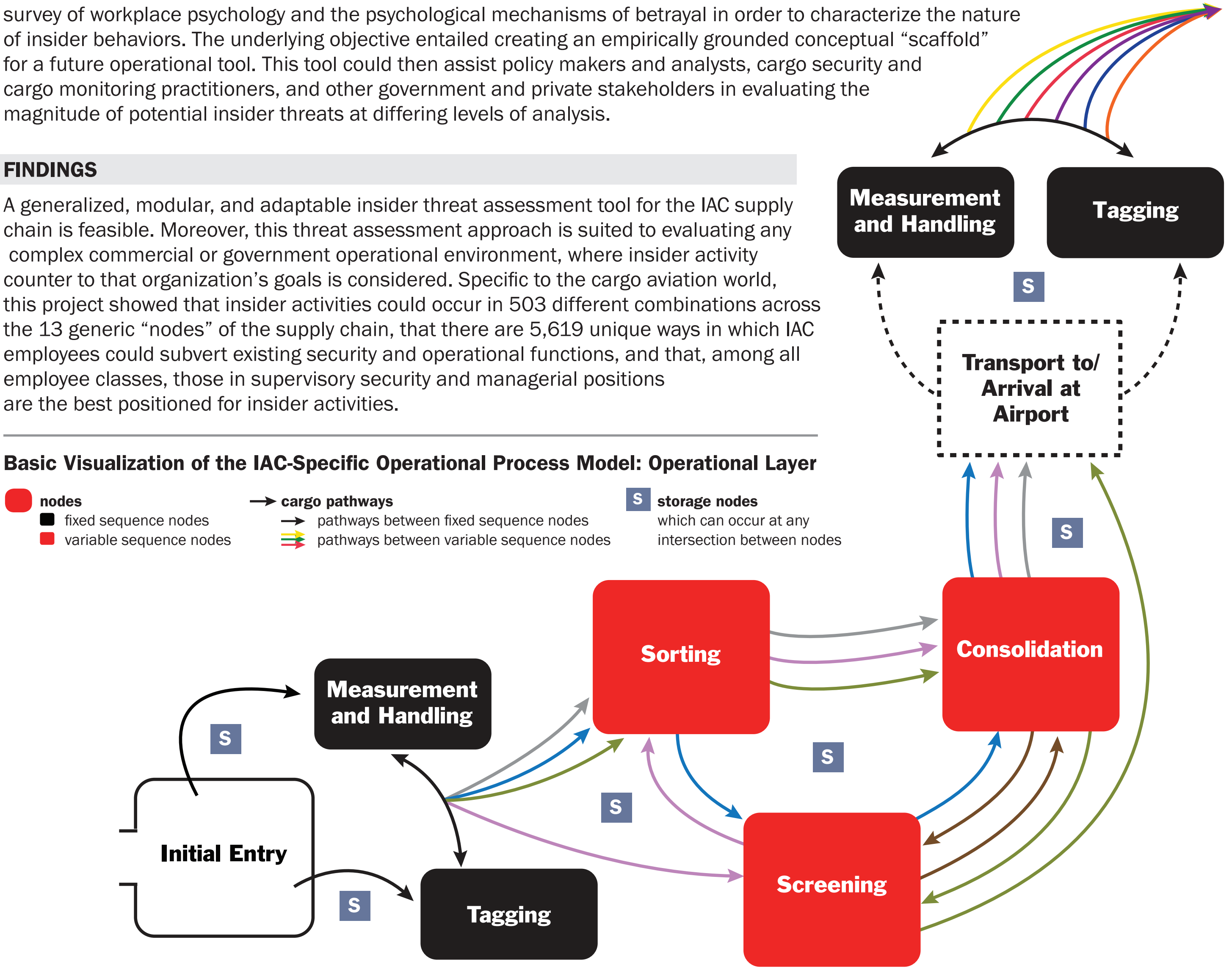
PROJECT BACKGROUND

This study was designed to analyze actors within the International Air Cargo (IAC) supply chain, in terms of their abilities to conduct insider threat activities within the operational environment. The study focuses on the possible facilitation of a plot planned and executed by an adversary without existing access to the supply chain and its choices in attempting to develop access through an insider, or an individual with legitimate access to a cargo environment, who would then act counter to commercial and security operations for the sake of the hypothetical plot. Such analysis requires an assessment of each operational phase and an evaluation of: a) the deterrent value of existing security and safety measures; b) existing regulatory frameworks and business systems; c) the identification of points in the chain where enhancements are needed to reduce insider threats; and d) an applied survey of workplace psychology and the psychological mechanisms of betrayal in order to characterize the nature of insider behaviors. The underlying objective entailed creating an empirically grounded conceptual "scaffold" for a future operational tool. This tool could then assist policy makers and analysts, cargo security and cargo monitoring practitioners, and other government and private stakeholders in evaluating the magnitude of potential insider threats at differing levels of analysis.

FINDINGS

A generalized, modular, and adaptable insider threat assessment tool for the IAC supply chain is feasible. Moreover, this threat assessment approach is suited to evaluating any complex commercial or government operational environment, where insider activity counter to that organization's goals is considered. Specific to the cargo aviation world, this project showed that insider activities could occur in 503 different combinations across the 13 generic "nodes" of the supply chain, that there are 5,619 unique ways in which IAC employees could subvert existing security and operational functions, and that, among all employee classes, those in supervisory security and managerial positions are the best positioned for insider activities.

Basic Visualization of the IAC-Specific Operational Process Model: Operational Layer

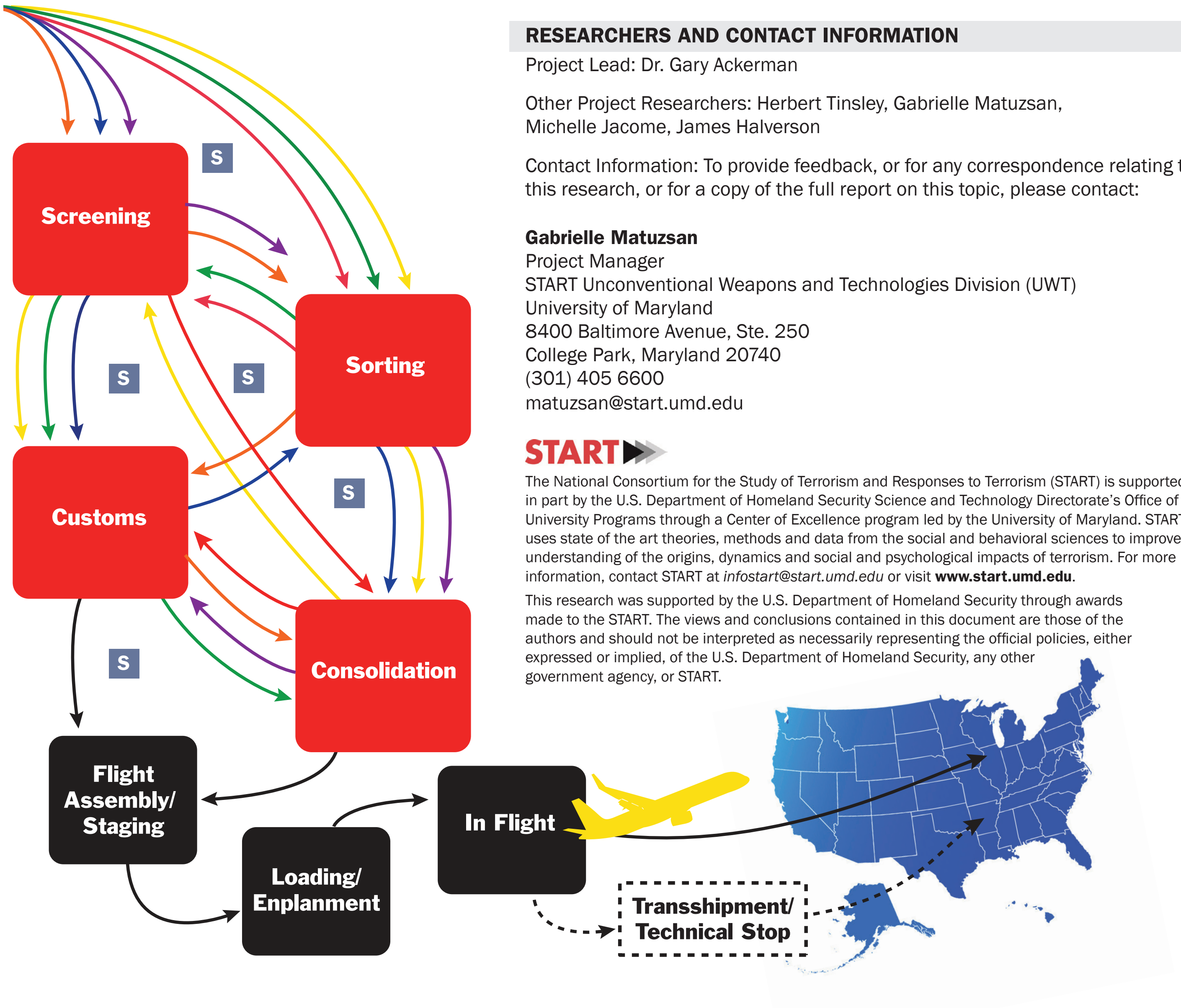

nodes
■ fixed sequence nodes
🟥 variable sequence nodes
→ cargo pathways
→ pathways between fixed sequence nodes
→ pathways between variable sequence nodes
S storage nodes
which can occur at any intersection between nodes
Measurement and Handling
Tagging
S
Transport to/ Arrival at Airport
S
Sorting
Consolidation
Measurement and Handling
S
S
S
Initial Entry
S
Tagging
Screening

METHODOLOGY

This study was approached through a five-fold methodology between December 2013 and May 2015. Researchers first conducted an extensive literature review covering air cargo supply chain and operations, aviation security, infiltration into legitimate organizations, corporate espionage and the psychology of betrayal and workplace psychology. Next, the research team interviewed 17 subject matter experts representing the fields mentioned above and engaged with various government and air cargo industry organizations—which involved visits to three domestic operational environments. Researchers conducted a week-long observational case study at Cargo City Bogotá-El Dorado International Airport, as guests of the Colombian civil aviation authority. Throughout these efforts, investigators built an operational process prototype, which provided a generic, spatial model of the air cargo supply chain and became the backbone for analyzing relationships between employees, security measures, insider activities, and cargo operations. The model incorporates an operational layer (where cargo movements are processed), a human activity layer (where security measures and various classes of employees interact to convey cargo items), and a threat layer (which delineates a typology of insiders and provides an adversary threat calculus for the potential insider and the external adversary seeking to illicitly transport RN weapons or materials). The team developed this model over three iterations, building upon the prototype as they proceeded. The final step involved development of an eight-step insider threat assessment procedure, useful for any application between basic possibility space analysis and extremely refined and data-rich analyses of specific air cargo environments.

FUTURE DIRECTIONS

START has received funding to extend the operational process model and threat assessment procedure by implementing them into a software tool that can be employed by a variety of end-users. Along with designing and developing this tool, researchers will direct efforts to validate the tool and its underlying algorithms, and conduct one domestic and two foreign use-cases, in order to collect data on the tool's performance in practical application. The resulting tool will be sufficiently flexible to be employed by government and private air cargo industry stakeholders. START will also engage with the nuclear industry, the maritime cargo industry, and other industries with sensitive security concerns in order to reconfigure the tool in order to evaluate insider threat potentialities in these fields.



RESEARCHERS AND CONTACT INFORMATION

Project Lead: Dr. Gary Ackerman

Other Project Researchers: Herbert Tinsley, Gabrielle Matuzsan, Michelle Jacome, James Halverson

Contact Information: To provide feedback, or for any correspondence relating to this research, or for a copy of the full report on this topic, please contact:

Gabrielle Matuzsan
Project Manager
START Unconventional Weapons and Technologies Division (UWT)
University of Maryland
8400 Baltimore Avenue, Ste. 250
College Park, Maryland 20740
(301) 405 6600
matuzsan@start.umd.edu

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is supported in part by the U.S. Department of Homeland Security Science and Technology Directorate's Office of University Programs through a Center of Excellence program led by the University of Maryland. START uses state of the art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, contact START at *infostart@start.umd.edu* or visit **www.start.umd.edu**.

This research was supported by the U.S. Department of Homeland Security through awards made to the START. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, any other government agency, or START.