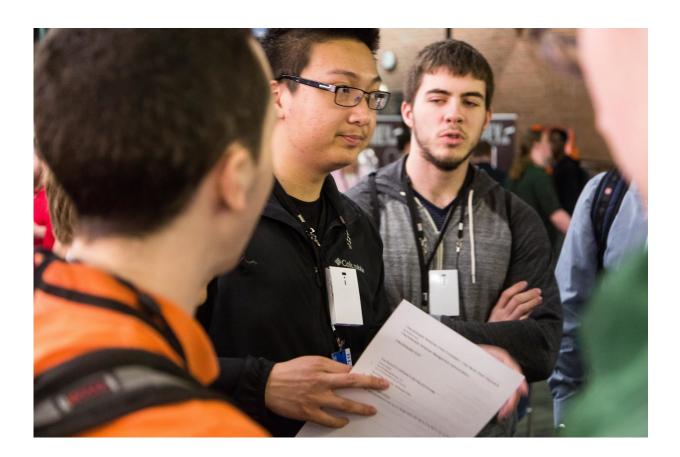# Cybersecurity teams that don't interact much perform best

April 27 2018

Members from the University of Maryland Baltimore College Cyberdogs wearing sociometric badges used to record how close each member is to each other and how much face-to-face communication they have. Credit: National Cyberwatch Center

Army scientists recently found that the best, high-performing

cybersecurity teams have relatively few interactions with their team-members and team captain. While this result may seem counterintuitive, it is actually consistent with major theoretical perspectives on professional team development.

"Successful cyber teams don't need to discuss every detail when defending a network; they already know what to do," said Dr. Norbou E. Buchler, team leader with the U.S. Army Research Laboratory's Cyber and Networked Systems Branch

In a recent study, "Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition" published in the latest issue of the *Journal of Computers & Security* scientists from the ARL, the National Cyberwatch Center and Carnegie Mellon University examined how collegiate cyber defense teams coordinate to mount and conduct an effective cyber defense during head-to-head team competition at the Mid-Atlantic Collegiate Cyber Defense Competition.

These teams were scored on four performance metrics while they attempted to defend their network against a cyber-attack campaign designed to disrupt critical U.S. infrastructure: maintaining networked services, responding to scenario events, assigned tasks by a role-playing chief executive officer and submitting incident reports to authorities.

Army researchers made use of Sociometric Badges (Humanyze Inc.), a sensing and recording device that students wore on a lanyard hanging from their neck. These badges collected data on a number of dimensions; the most valuable being face-to-face interactions between team members (via infrared sensors). In addition, Army researchers developed a questionnaire to measure the leadership style, task distribution, team meetings, communication and collaboration based on the opinions of the observers assigned to each team.

Teams with effective leadership and functional specialization within the team were more successful. Face-to-face interactions, as measured by the sociometric badges, emerged as a strong negative predictor of success in the competition, explained Buchler, a cognitive scientists within ARL's Human Research and Engineering Directorate.

Members of the University of Maryland Baltimore College Cyberdogs team primarily focus on working rather than interacting. This fits with US Army Research Laboratory findings as this was the highest performing team at this event, according to Claire le Fleur, an Army researcher. Credit: National Cyberwatch Center

"In other words, the teams whose members interacted less during the

exercise, were usually more successful," Buchler said.

He said the results demonstrate that human collaboration and leadership of cybersecurity teams are essential when responding during a realistic cyber-attack.

"These results are important because current training programs commonly emphasize cyber security knowledge and do not provide training on effective team management," he said.

"The research also demonstrated the value of measures derived from recent advancements in wearables technology by capturing face-to-face interactions. Increasingly, such social sensing platforms are being leveraged by Army researchers, industry and academia to enhance human measurement and validate and refine theories regarding the factors influencing human performance and teamwork over time," Buchler said.

"High-performing teams exhibit fewer team interactions because they function as purposive social systems, defined as people who are readily identifiable to each other by role and position and who work interdependently to accomplish one or more collective objectives," continued Buchler, who referenced Tuckman's model in this understanding. "The responsibility for performing the various tasks and sub-tasks necessary to accomplish the team's goal is divided and parceled-out among the team."

The research team is part of the Army Research Laboratory's Cybersecurity Collaborative Research Alliance seeking to advance a foundational science of cybersecurity that addresses the human dynamics of attacker, defender, and user interactions to support training effectiveness and improve the operational efficiency and effectiveness of cyber operations.