On Thursday, September 17, 2020, Constitution Day, the Cybersecurity Strategy and Information Management Program at The George Washington University in partnership with CSFI and the Economic and Trade Office at the Israeli Embassy in Washington, D.C. hosted a panel event entitled *"The Conduct of Cyber Enabled Information Operations."*

The event opened with a short CSFI video depicting a fictitious, but realistic scenario. A terrorist group working with sophisticated, international hackers launched a multi-faceted cyber campaign aimed at undermining western democratic principles and election security. By manipulating social media messaging and injecting content into media and news stations, the terrorists sought to impact public perceptions of U.S. leaders and candidates for local, state and national elections and to instill doubt regarding the reliability of the U.S. voting process. To add further confusion and panic during the weeks leading up to the election, the hackers flew drones that dusted fake white (anthrax-like) powder over polling sites.

The implications of this type of attack are significant. Elections are an essential part of a democratic and free society. The outcomes of a national election can shape the strategic trajectory and can impact other nations in significant ways. With the increase in the scope and scale of cyber attacks and influence operations, determining effective ways to deter and counter them is and will continue to be a necessary step in maintaining national and global security.

At the conclusion of the video, a group of distinguished panelists discussed these issues as well as challenges related to deception, disinformation, cyberspace operations, and election security. They also examined the use of social media as a tool to disrupt the ability to lead or direct operations.

EVENT PARTNERS

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

THE CYBERSECURITY FORUM INITIATIVE

Trade & Economy

Israeli Embassy Washington, DC

Noting that the U.S. is involved in daily, persistent cyber engagement just under the threshold of war, the panelists warned that other countries are in a very real competition with the U.S. in cyberspace and have sought to shape U.S. perceptions and beliefs about a variety of topics.

> ***"We have come to realize that adversarial nations can hack more than our networks. Our competitors are using cyberspace to attack our democratic processes, to, in essence hack our minds and culture."***
>
> ***- Harry Wingo***

The panel also discussed other ways that adversaries could potentially impact human behavior and perception. Rear Admiral Danelle Barrett discussed some of the opportunities and challenges surrounding technological advances related to human-machine interfaces. Retired Rear Admiral Becker and Brigadier General Touhill (retired) addressed a handful of thoughtful comments and questions from the audience members regarding principals related to cyber warfare and the potential use of cyber to impact the hearts and minds of citizens during battle. Lastly, some current technology and processes available to address security challenges were also examined. Ira Hoffman reminded participants of some of the legal ramifications related to cyber intrusions.

In response to audience questions about how to protect against online propaganda and misinformation, panelists cautioned audience members to employ critical thinking and to seek a variety of sources to gather their news. Brett Feddersen noted that "Knowledge from like minded sources will shield you from the truth. Understanding diversity can protect you from cyber-enabled influence campaigns and reveal fact from fiction"

Johnmichael O'Hare reinforced the need for collaboration among public, private corporations and with international partners to solve some of these emerging security challenges. Having good relationships with allies and like-minded partners is one way to prevent strategic surprise and strong diplomatic ties can minimize the capacity for an adversary to gain an initiative. In particular, Josh Cohen shared that, "the Economic and Trade Office at the Israeli Embassy was really excited to be part of this event and have a leading Israeli cyber Intel company participate. Its activities like these that demonstrate the US-Israeli relationship across multiple fields, including cyber, remains very strong."

Harry Wingo summarized the event as follows, "I was inspired by the expertise of the panel members, and particularly by the insights they shared on great power competition in the area of cyber enabled information operations. We have come to realize that adversarial nations can hack more than our networks. Our competitors are using cyberspace to attack our democratic processes, to, in essence hack our minds and culture. Anyone who attended the session was treated to useful perspectives from some of the best experts in the field. I was honored to be part of this event." ◆

EVENT PARTICIPANTS

OPENING REMARKS

CONNIE UTHOFF, Associate Director, GW's Cybersecurity Strategy and Information Management (CSIM) Master's Program

CHRISTINE DE SOUZA, CSFI Director, Cyberspace Operations Strategist at SOS International LLC, and USAF Cyber Warfare Operations Officer

JOSHUA COHEN, Trade and Partnership Director, Economic & Trade Office at the Embassy of Israel, Israel Trade & Economic Mission in Washington, DC

MODERATOR

HARRY WINGO, J.D., Professor at National Defense University, Former Navy SEAL officer, and United States Naval Academy Graduate

DISTINGUISHED PANELISTS

REAR ADM. DANELLE BARRETT, USN (Ret.), Former U.S. Navy Cybersecurity Division Director and Deputy Chief Information Officer, and CSFI Advisory Director

BRETT J. FEDDERSEN, President at AcceleratUM; Former Acting Director for National Security Programs and Incident Response, the Federal Aviation Administration; Former Principal Deputy Director for Transregional Threats, the Department of Defense; Former Director for Transportation and Border Security, The National Security Council, Executive Office of the President

DISTINGUISHED PANELISTS *(cont'd)*

JOHNMICHAEL O'HARE, Director, Sales and Business Development (COBWEBS)

ROY HELLER, Chief Operations Officer at Nucleon Cyber and Cyber Intelligence SME

REAR ADM. PAUL BECKER, U.S. Navy (Ret.), Former Executive Office of the President at The White House, Presidential Transition Team's Intelligence Community, former Chairman of the Joint Chiefs of Staff, Director for Intelligence (J2), CEO at The Becker T3 Group LLC, and CSFI Advisory Director

BRIG. GEN. GREG TOUHILL, USAF (Ret.), President at AppGate Federal Group, Former United States Government's Chief Information Security Officer, Former Deputy Assistant Secretary for Cybersecurity and Communications in the U.S. Department of Homeland Security and as Director of the National Cybersecurity and Communications Integration Center, and CSFI Advisory Director

IRA HOFFMAN, CyberSecurity Attorney at Butzel Long and CSFI Senior Fellow