RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: EXP-T07

CYBERWAR GAME: BEHIND CLOSED DOORS WITH THE NATIONAL SECURITY COUNCIL

Moderators:

Dmitri Alperovitch
Co-Founder and CTO, CrowdStrike
@DAlperovitch

Jason Healey
Senior Research Scholar, Columbia University SIPA
@jason_healey

RSAConference2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: EXP-T07

CYBERWAR GAME: BEHIND CLOSED DOORS WITH THE NATIONAL SECURITY COUNCIL

Panelists:

John Carlin
Partner and Chair, Global Risk & Crisis Management
Morrison & Foerster LLP

Eric Rosenbach
Co-Director, Belfer Center for Science and International Affairs, Harvard Kennedy School

Joan O'Hara
Acting National Security Advisor, Vice President of the United States

Suzanne Spaulding
Senior Adviser, Homeland Security Program and International Security Program
Center for Strategic and International Studies
@SpauldingSez

The Situation #1

Monday, 11 June 2018

- US intelligence has uncovered additional military dimensions of the Iranian nuclear program.
- Iran has refused access to inspectors which the US government believes it must under the Joint Comprehensive Plan of Action.
- The Trump administration also notes long-standing issues including:
  - Continuing missile tests by Iran and support for Assad's war crimes in Syria
  - Support for Houthi rebels in Yemen as well as launching of missiles against Saudi Arabia
  - Continued aggression against Israel by way of sponsoring Hezbollah, Hamas and other proxies
  - Continued hacking against Saudi Arabia, aiming to destroy physical infrastructure
- Accordingly the Trump Administration announced that it was accordingly withdrawing from the JCPOA, will snap-back sanctions, and execute "military remedies."

The Situation #1

Wednesday, 13 June 2018

- With the JCPOA collapse, Iran declares it now have to consider, for the first time since the Glorious Revolution of 1979, **pursuing a nuclear weapons program**. They reaffirm their right to continue development of long-range ICBMs.
- **Immediate and furious new series of cyber campaigns**.
  - Leaked documents from previous intrusion into House of Representatives and Senate and destroys the networks with a crude wiper attack.
  - Leaked documents from previous intrusions into major US-Israel interest groups in US.
  - Theft of $1.5 billion USD worth of currency from US financial institutions via direct intrusions into those banks and leveraging of the SWIFT network to issue transfers.
- US intelligence and law enforcement – and commercial threat intel companies – suspect **IRGC involvement** but cannot yet confirm.

The Situation #2

Friday, 15 June 2018

- US Intelligence Community **positively attributes** these cyber actions to **private contractors in Iran**, who SIGINT shows, have been tasked by IRGC to execute these operations.
- The attacks hit a new level with Iranian operators:
  - Stepping up intrusions into Israeli critical infrastructure assets and causing localized power outages. Electricity remains uninterrupted to most of the country.
  - Compromise the subway control system of the Los Angeles subway system, disabling the signal control system, which forced one train to crash into another waiting on the platform during the Friday afternoon rush hour. Media reports unconfirmed fatalities.
  - Intelligence believes Iranians may have access to other metropolitan transportation systems in the US and UAE.