RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PNG-F02

Behind the Headlines: A Public-Private Discourse on Cyber Defense

MODERATOR: **Theresa Payton**
CEO and Founder, Fortalice Solutions
@FortaliceLLC @TrackerPayton

PANELISTS: **Curtis Dukes**
EVP & GM, Security Best Practices & Automation Group, CIS

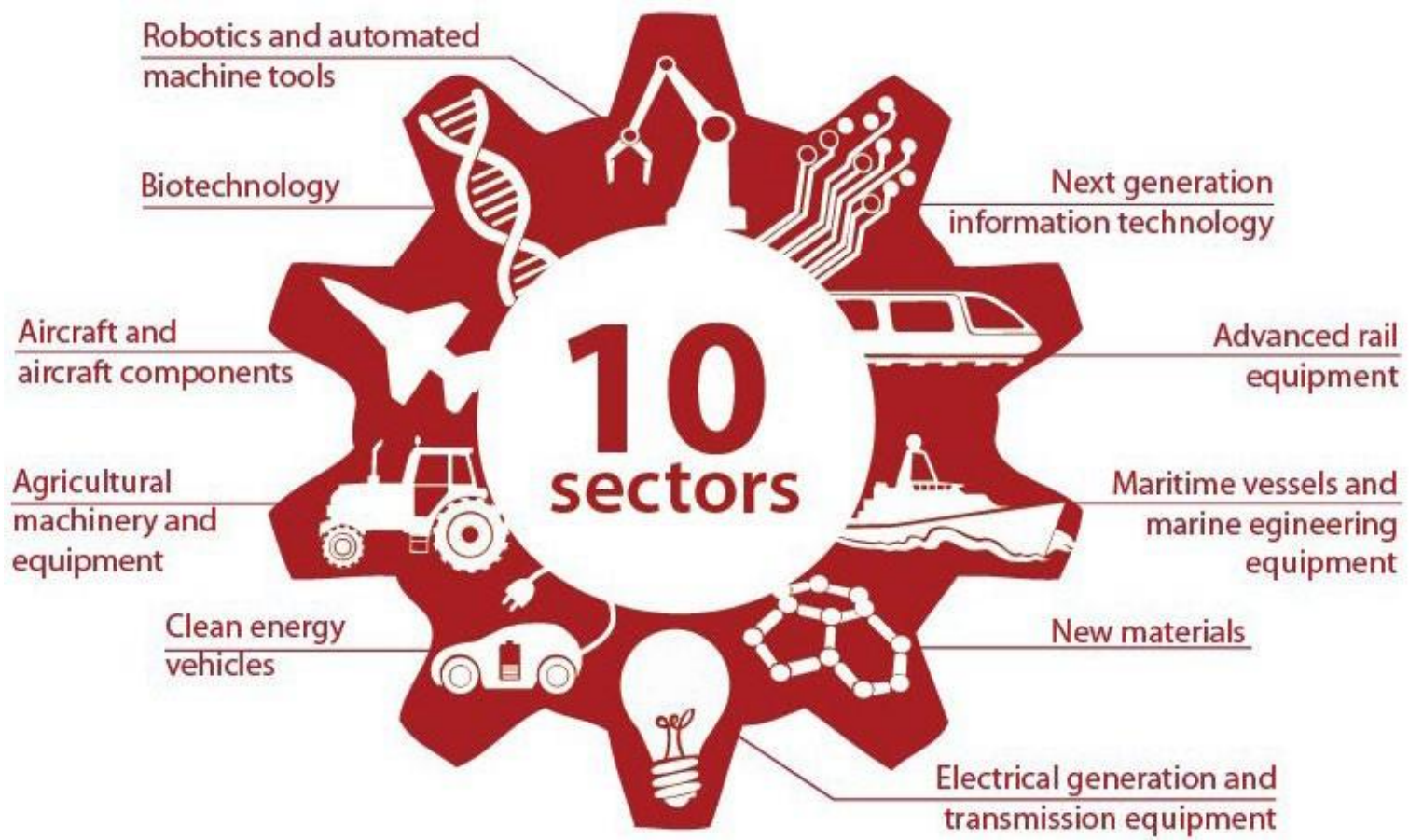
John Felker
Director, NCCIC, CISA DHS

Neal Ziring
Technical Director, Capabilities Directorate, NSA

THREATS FROM THE TOP FOUR

CHINA - MSP

- Continues digital economic espionage even after 2015 cyber agreement to stop



THREATS FROM THE TOP FOUR

IRAN - DNS Hijacking

- Interested in non-oil Industries to grow economy
- Targeting U.S. government and companies for intel to posture for future cyber operations

https://resources.infosecinstitute.com/attacks-over-dns/

THREATS FROM THE TOP FOUR

RUSSIA - VPNFilter

- Needs to bolster economy (corruption, state control, loss of cyber talent)
- Global intel collection and info ops
- Putin orders Russia to unplug from the Internet in event of war

THREATS FROM THE TOP FOUR

DPRK

- Needs to develop domestic IT infrastructure and industry
- Ransomware funds regime
- Has militarized IT infrastructure
- Isolated; virtually hack-proof to retaliation

www.dailystar.co.uk

MITIGATION and TAKE AWAYS

- Cyber hygiene and best practices
- Information exchange and collaboration
- Baseline risk (MITRE ATT&CK or similar framework)
- Evolve defenses against cyberattack complexity
- Exercise risk/incident response with entire organization

RSAConference2019

Behind the Headlines: A Public-Private Discourse on Cyber Defense