



Cyber Trends

A 10-Year Forecast

© 2008 Science Applications International Corporation. All rights reserved. SAIC, the SAIC Logo, and "Science to Solutions" are trademarks or registered trademarks of Science Applications International Corporation in the United States and/or other countries.





Examine the cyber-environment in October 2019

- Technology
- International environment
- National security
- Federal civilian and Comprehensive National Cybersecurity Initiative (CNCI) 3

Technology in 2019



- Mobile platforms
- Quantum computing
- Cloud
- Web 3.0
- Death of the perimeter; reduction of dependence on malware signatures
- Emphasis more on protecting data/services versus transport

International Environment in 2019



- International law enforcement agreements greatly facilitate e-crime mitigation
- Chinese digital legal regime finally in place after government loses control of state-nurtured hacktivism. First two generations of hacktivists turned to criminal hacking as the People's Republic of China (PRC) Internet economy matured.

Federal Civilian in 2019



- Cyber coordinator at National Security Council – but...
- Strong Department of Homeland Security (DHS) lead for .gov and critical infrastructure
 - DHS lead agency for standards and situational awareness
 - Minimal regulatory environment
- Information-sharing barriers between public/private sectors greatly reduced, yet interagency and federal/state/local sharing remains problematic
- With the advent of cloud, we have realized that the aggregation of data and services have created a national vulnerability – creating a new digital sector in the National Critical Infrastructure Strategy

National Security in 2019



- Convergence of offense, defense and intelligence, but...
- U.S. government network intelligence will largely derive from commercial sources and technologies. Shared situational awareness dependent on commercial sector
- Cyber deterrence as a doctrine largely discarded as unworkable
- Cyber Command will remain principally a supporting command in support of Regional Combatant Commands
- The countries that master the virtual/physical bridge control the battlefield



- Third generation of the Comprehensive National Cyber Security Initiative (CNCI 3). Focus is on data protection and integrity and on national identity management
- The Civil Rights Act of 1964 is amended to establish the Privacy and Civil Liberties Commission. Chartered to investigate violations of U.S. person's privacy and civil liberties in the digital age
- Concept of needing a good (cyber) offense in order to have a good defense is thrown on the ash heap of “good aphorisms but bad ideas”
- Cybersecurity education is considered a national imperative and the foundation for cybersecurity

The National Cybersecurity Operations Concept 2019



NTOC

CYBERCOM

US-CERT

**Critical
Infrastructure**

NTOC = National Security Agency/Central
Security Service Threat Operations Center

CYBERCOM = Cyber Command

US-CERT = United States Computer
Emergency Readiness Team

NCIJTF = U.S. National Cyber Investigative
Joint Task Force

NCIJTF



Questions or comments?

Contact: Robert Giesler; “robert.j.giesler@saic.com”