

Commonwealth of Virginia Cyber Commission

Town Hall - Virginia Tech

24 February 2015

---

# A CISO's Perspective...

J.C. Dodson

Virginia Cyber Security Commissioner

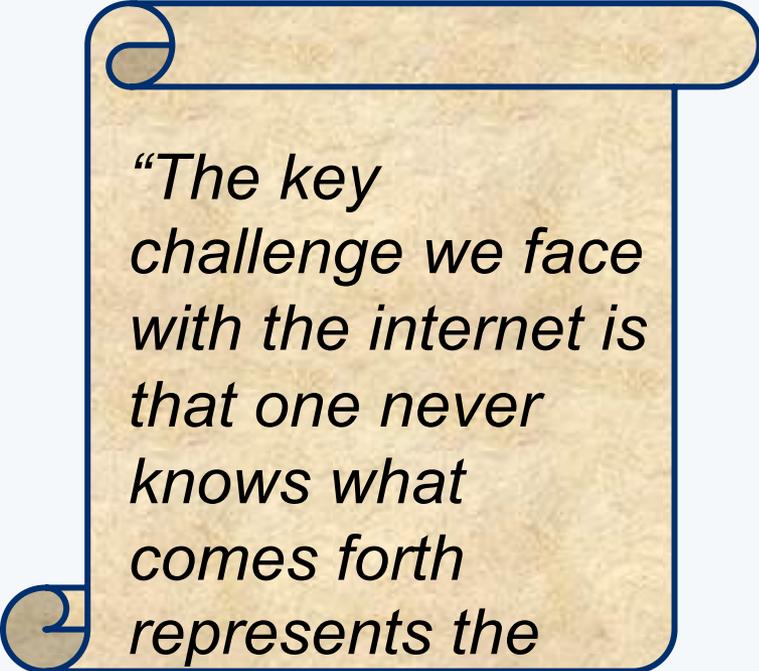
Vice President, Global Chief Information Security Officer (CISO)

BAE Systems

---

# Today's Discussion

- Environment
- Risk Construct
- Challenges
- Way Forward Considerations



*“The key challenge we face with the internet is that one never knows what comes forth represents the truth.”*

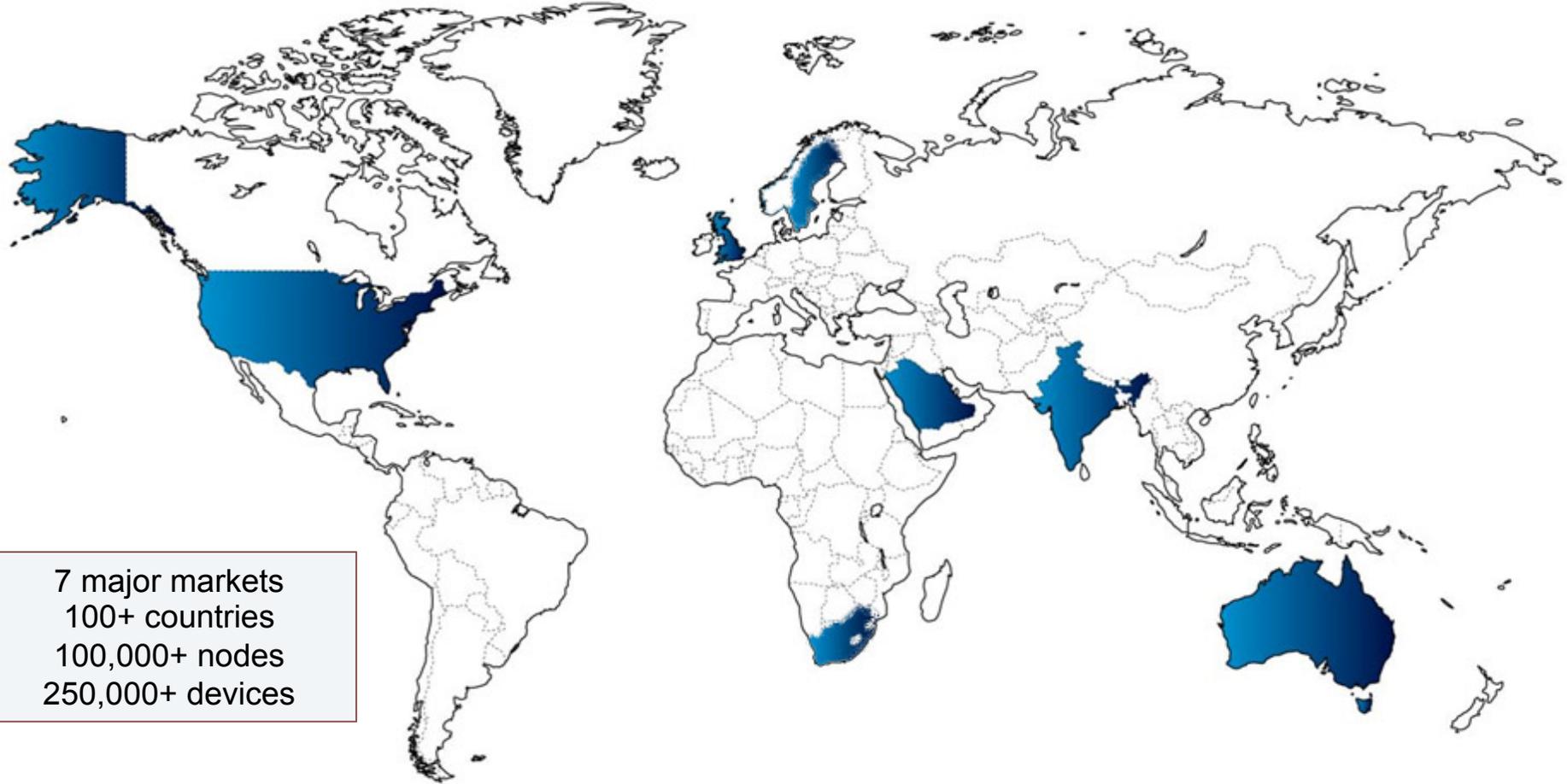
- Thomas  
Jefferson

# Our Digital Environment...

---

- Every 10 minutes these days, mankind creates as much information as the first 10,000 generations of human beings did
- Every minute in 2014, we sent about 204 million emails, ran 2 million Google searches, tweeted 100,000 times, downloaded 47,000 apps from the Apple app store, and uploaded 48 hours of new video to YouTube
- Up to 200,000 new viruses are created each day, and the average anti-virus software stops just 5 percent of malware
- United Nations estimates that transnational organized crime rakes in more than \$2 trillion a year in profits--that accounts for 15-20% of global GDP
- About 90 percent of small businesses that have customer information stolen go out of business within three years of an attack
- Medical identity theft — false claims with stolen IDs — cost the U.S. healthcare system \$5.6 billion annually

# BAE Systems' Global Cybersecurity "Footprint"



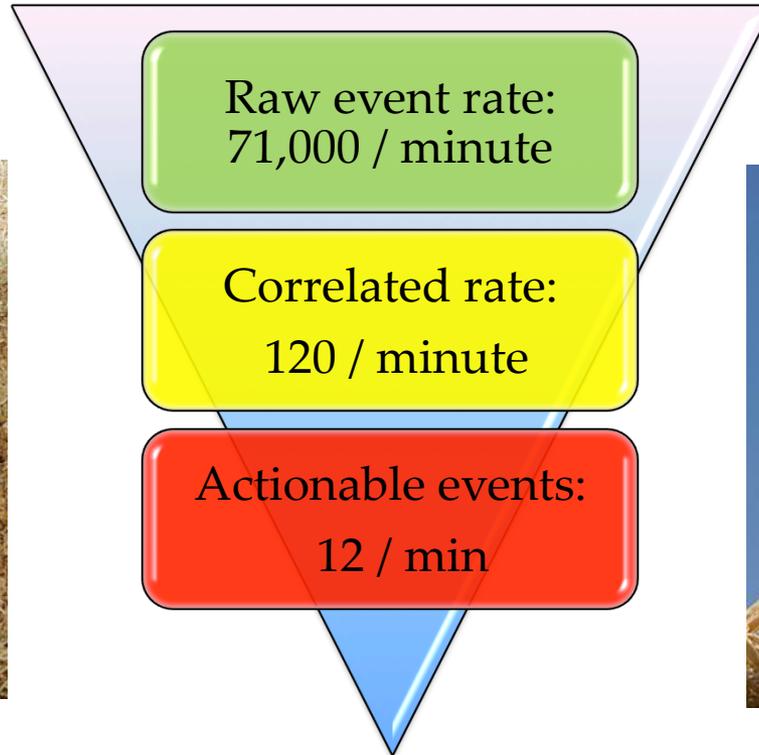
Multi-national computer network defense team spanning 16 time zones

# CISO “Job Jar”

- Advise Chief Executive and Board on cybersecurity risk mitigation posture
- Corporate computer network defense – intelligence, analysis & engineering
- Identity access management – who & how
- Investigations and forensics – due process & legal sufficiency
- Cybersecurity policy and employee knowledge
- Daily management of “healthy” tensions
  - Collaboration vs control
  - New technology adoption vs undefined exposure
  - Individual risk appetite vs collective risk appetite
  - Positive user experience vs security labyrinth

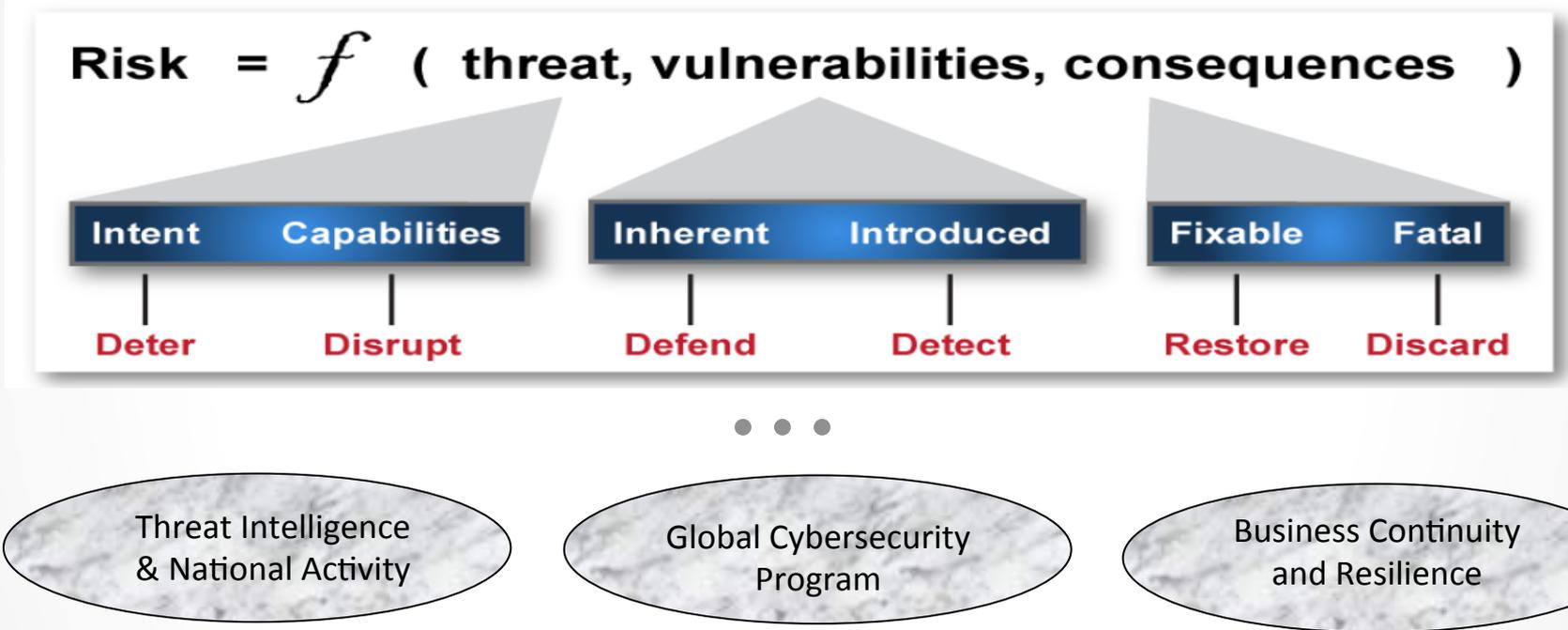
Translate complex risk positions – contain ambiguity – trade-off action / in-action

# “Secret Sauce:” Finding Information Amongst Noise



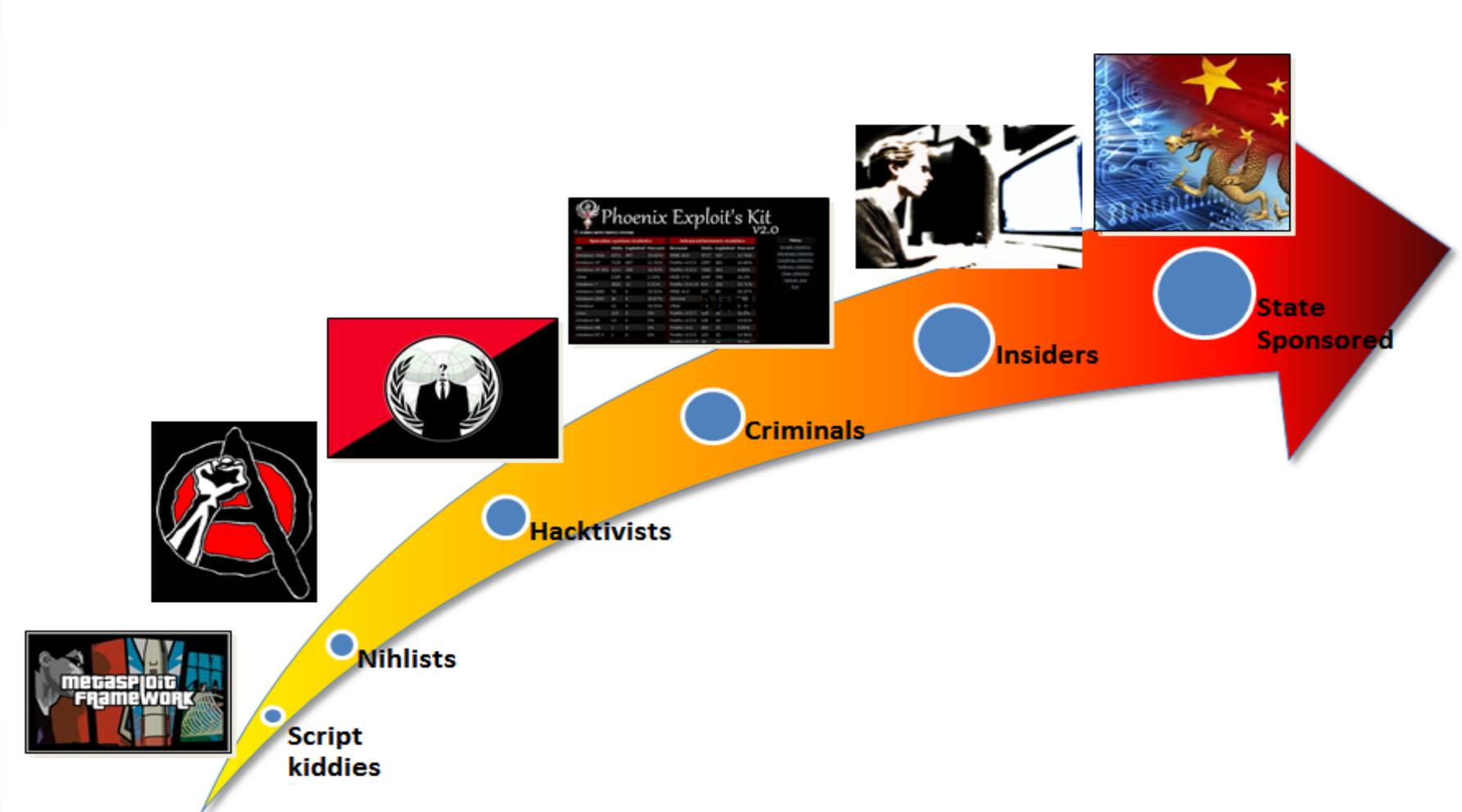
Analyzing over 10 billion logs/month — advanced persistent threat detection

# Global Cybersecurity Risk Construct



**Minimize corporate risk exposure and business impact – increase ability “to take a punch”**

# Threat Actors & Risk



Targeted and non-targeted threats – unique tactics, techniques & procedures

# Strategic Challenges

- ❑ Migration of threat from theft, to the “4Ds” (disrupt – deny – deceive - destroy)
- ❑ Host nation policies: authority / accountability / liability / privacy
- ❑ Global supply chain exposure and risk ownership
- ❑ Shareholder valuation – reputation, M&A, insurability
- ❑ Industry’s authority / role in “active defense”
- ❑ Expansion to cloud /mobility / BYOD / work & personal data mix



Convergence of national issues and corporate risk management approach

# Way Forward Considerations

- Knowledge and informed decision making – educate – educate - educate
- Ownership at each level: individual, local, state, federal, international
- Embrace basic standards of compliance
- Information sharing w/o litigation exposure
- Balance risk control & resilience efforts
- Raise the fence – increase the deterrence



Collaboration and sharing of threat / response information is optimum lever