THE EVOLVING CYBER THREAT LANDSCAPE :
Ensuring the Integrity and Value of Information

Sean Kanuck
Director of Cyber, Space and Future Conflict
The International Institute for Strategic Studies

NATO Parliamentary Assembly
Warsaw, Poland
27 May 2018

“ In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed. ”

Director of National Intelligence
Worldwide Threat Assessment
26 February 2015

“ Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) … ”

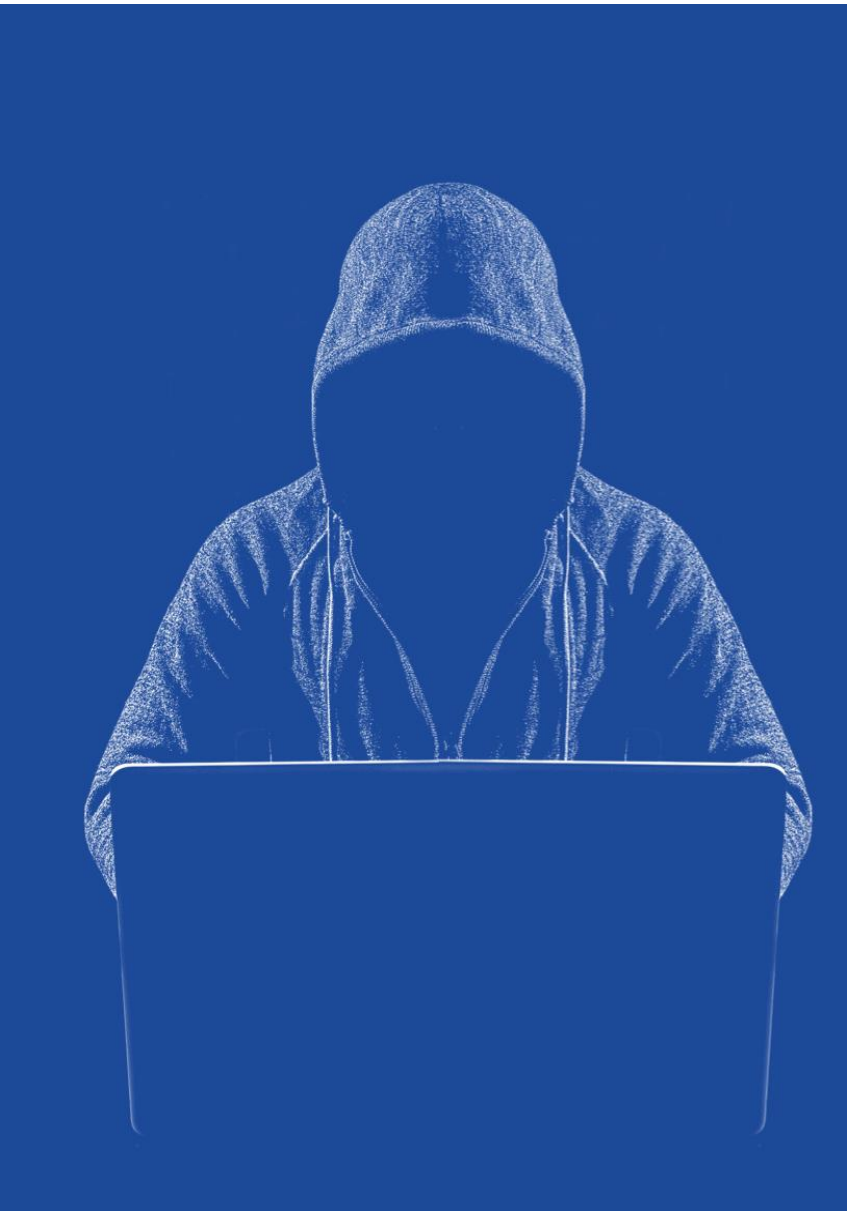
Director of National Intelligence
Worldwide Threat Assessment
9 February 2016

Functionality ≠ Security

People + Processes + Technology

Offense > Defense

Interests ↔ Actions ↔ Incentives



STRATEGIC TRENDS

Intervention -- offensive operations below level of armed conflict

Industry -- private sector companies are enablers, targets, and victims

Infrastructure -- automation, lower resiliency, higher volatility

Indirect -- opportunism, collateral damage, cascading effects

Integrity -- data manipulation and fabricated information campaigns

SALIENT MILESTONES (2016 – 2018)

Fake News -- Russian influence operations and social media

Fake Crime -- WannaCry / NotPetya disrupted systems worldwide

Real News -- EU data regulation, Equifax, and Meltdown / Spectre

Real Crime -- US Securities and Exchange Commission disclosure

Realism -- UN Group of Governmental Experts lacked consensus

RISK ENVIRONMENT

technological convergence

increasing rate of change

upstream / downstream integration

cross-sectoral interdependence

IMPROVING RESILIENCE

assume compromised environment

recognize cumulative costs

avoid single “points” of failure

plan for cascading effects

IoT + AI = Potential Volatility

Threats to Data Integrity

FINANCIAL INSTITUTIONS

Fraudulent SWIFT transfers (Bangladesh, India)

INDUSTRIAL CONTROL SYSTEMS

European vendor software updates compromised

HEALTHCARE PROVIDERS

Ransomware attacks that alter rather than encrypt data

Threats to Information Integrity

DEMOCRATIC INSTITUTIONS

Fraudulently influence voter turnout and/or ballots

CAPITAL MARKETS

Misinform investors and/or regulators

PUBLIC SAFETY

Mass migration in India resulted from social media post

Technical Defense Measures

Biometric Identification	Authentication	Non-repudiation
Blockchain	Provenance	Verification
Artificial Intelligence	Detection	Deception
Quantum Encryption	Protection	Notification

Preserving Information Integrity

- Rigorously employ cyber security “best practices”
- Create additional resilience through redundancy in order to recover from adverse events
- Utilize a threat analysis model that adopts an attacker’s perspective of your organization and its external dependencies
- Develop a business strategy that is cognizant of information challenges and prepare contingency plans

Q & A