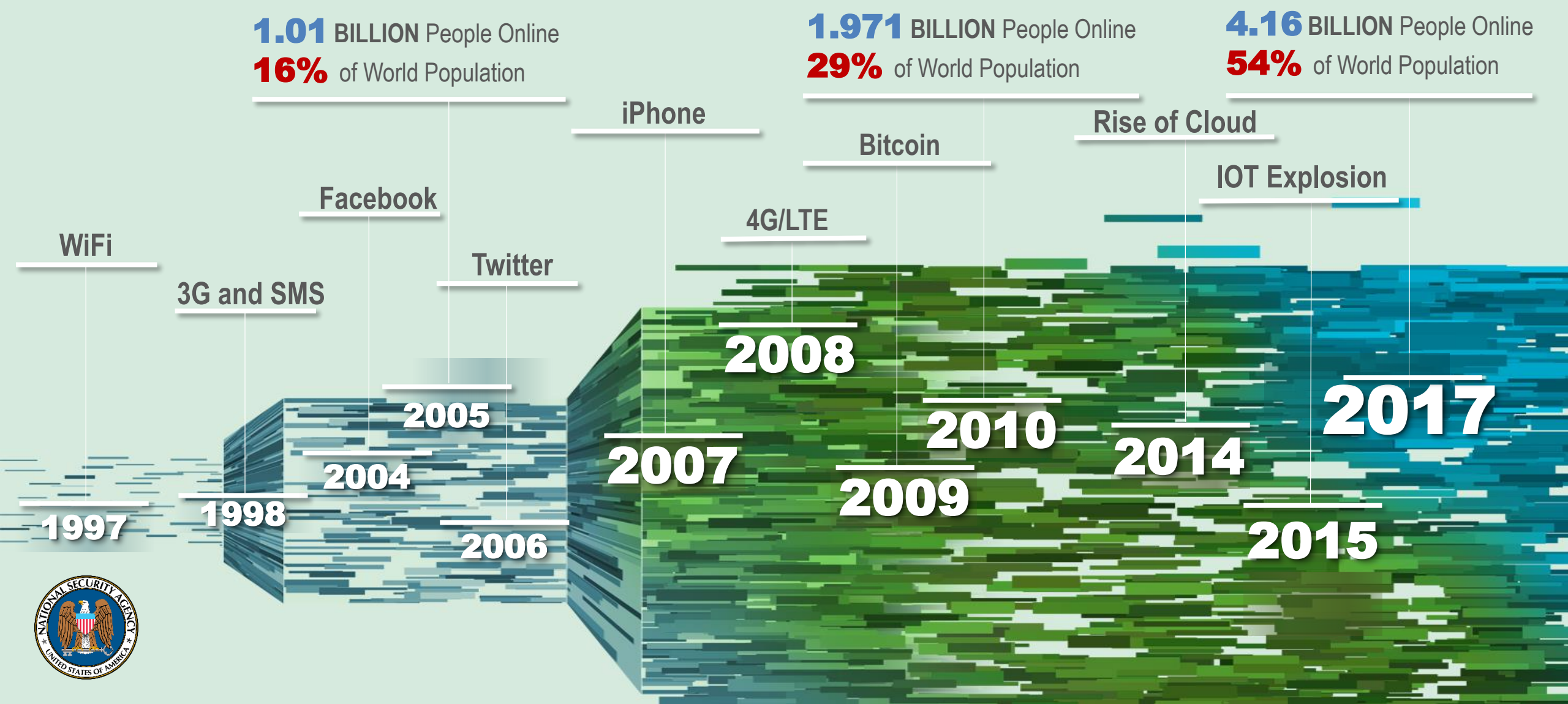
NSA TALKS CYBERSECURITY



Rob Joyce
Senior Advisor for Cybersecurity Strategy

Information Technology Game Changer



Escalating Cyber Events

2008-2011

Agent.btz found on DoD systems

Stuxnet impacts Iranian nuclear fuel enrichment

2012-2013

Saudi Aramco suffers data destruction attack on 30k machines

380+ Iranian DDoS attacks U.S. financial institutions

China Mandiant report on “APT1” details commercial IP theft and more

2014-2015

Iranian actors hit U.S. casino with destructive cyberattack

Chinese actors compromise OPM databases

Cyberattack against **Ukraine electrical grid**

2016-present

Russian Not-Petya attack on Ukraine propagates globally costing billions

DPRK WannaCry malware knocks out computers in 150 countries in under 24 hours

Russia Cyberattack on Pyeongchang Olympics took official Olympic website offline for 12 hours

Today's Cyber Threats

- High-End cyber threat activity continues to become **MORE SOPHISTICATED**
- The **LEVEL OF EXPERTISE REQUIRED IS DECREASING** as sophisticated internet tools become easier to use
- **TREND IS CLEAR:** moving from exploitation, to **DISRUPTION**
- **GROWING** use of **INFORMATION OPERATIONS** leveraging cyber intrusions

New Threat Environment



Cloud Based Services



Smartphones and
Internet of Things (IOT)



Big Data

HARD TRUTH: More technology used, more risk grows
Technology Debt is a serious problem

NSA's Unique Cybersecurity Mission

SIGNALS INTELLIGENCE

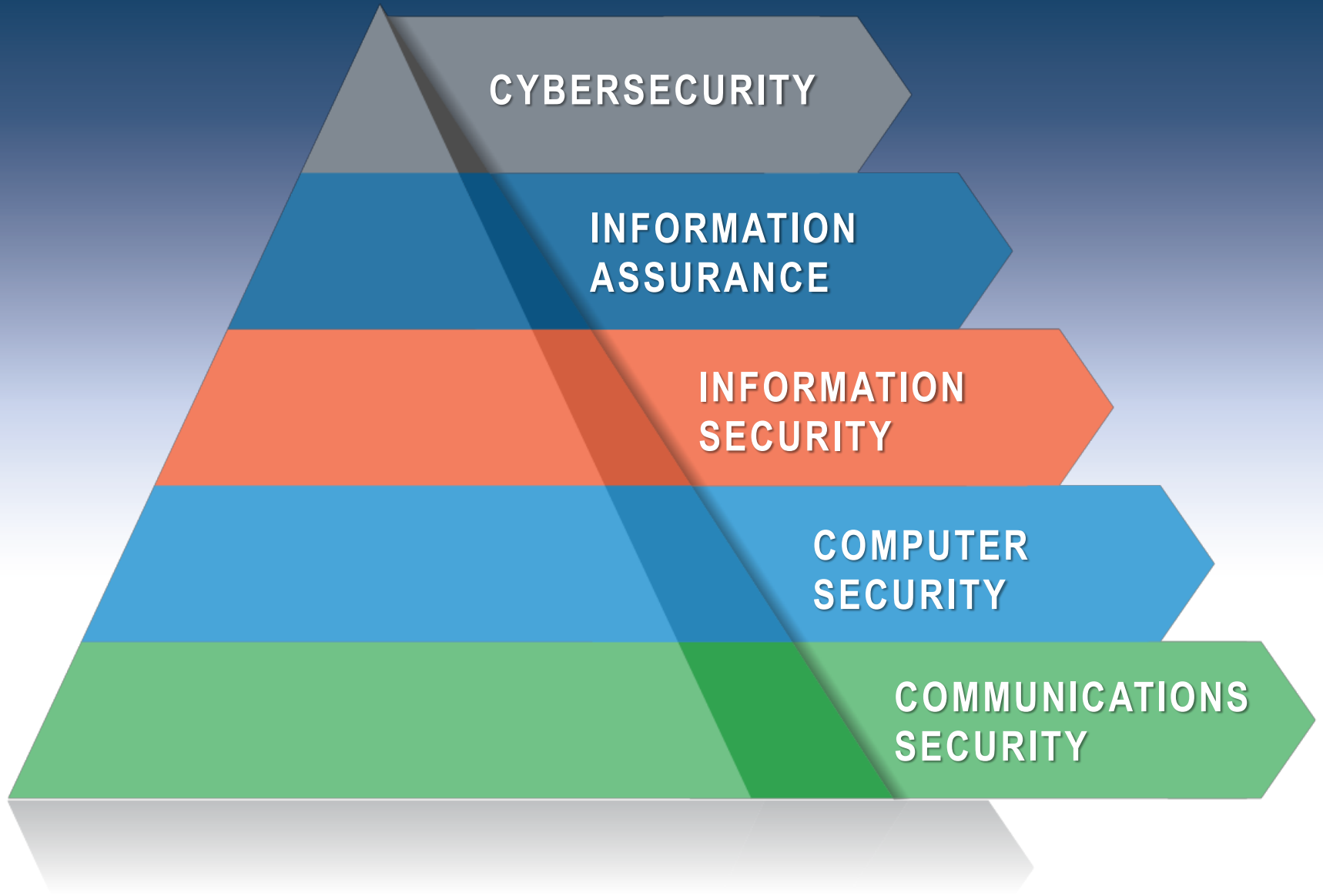
Intercept and exploit foreign signals



INFORMATION ASSURANCE

Defend National Security Systems

Cybersecurity Evolution at NSA



NATION STATE ACTIVITY

Almost every state has developed cyber capabilities.

A few are behaving much worse than others.



THE NEW NORMAL

FUNDAMENTAL SHIFT IN NATION STATE ACTIVITY

Geopolitical events have drastically altered the operating profile of sophisticated nation state adversaries.



THE NEW NORMAL

FUNDAMENTAL SHIFT IN NATION STATE ACTIVITY

Geopolitical events have drastically altered the operating profile of sophisticated nation state adversaries.



THE NEW NORMAL

FUNDAMENTAL SHIFT IN NATION STATE ACTIVITY

Geopolitical events have drastically altered the operating profile of sophisticated nation state adversaries.



THE NEW NORMAL

FUNDAMENTAL SHIFT IN NATION STATE ACTIVITY

Geopolitical events have drastically altered the operating profile of sophisticated nation state adversaries.



Defense is a Team Sport



WEAPONIZATION OF INFORMATION
goes beyond typical cybersecurity



NSA PARTNER
with DOD, FBI and others



LEVERAGE INTELLIGENCE AND EXPERTISE
to address threat



PROTECT AND SECURE INTELLIGENCE
vital networks (including elections)

Intrusion Lifecycle



- Reconnaissance
- Initial Exploit
- Establish Persistence/ Maintain Access
- Install Tools
- Move Laterally
- Collect, Exfil/ Exploit/Destroy

Cyber Defense Matters

WE KNOW WHAT WE NEED TO DO

- Patch Management
- Least Privilege Administration
- Multi-factor Authentication
- Know Your Network
- Daily Backups



- White Listing
- Enable Logging/ Do Analysis
- Harden – (Flash, Java, Microsoft Ole, Macros, Etc.)
- Data Encryption

NSA Top 5 Actionable SOC Principles

1 INSTITUTE **WELL-MANAGED** & **DEFENDABLE** PERIMETERS & GATEWAYS



2 ENSURE **VISIBILITY & CONTINUOUS MONITORING OF THE NETWORK** TO INCLUDE TRAFFIC & ENDPOINTS



3 **HARDEN NETWORKS, ENDPOINTS, & SERVICES** TO BEST PRACTICES



4 USE **COMPREHENSIVE** & **AUTOMATED** THREAT INTELLIGENCE SOURCES

5 **CREATE & FOSTER** A CULTURE OF **CURIOSITY** & EMBRACE **INNOVATIVE APPROACHES**





NEED CONFIDENCE IN
COMMERCIAL TECH

Modern Reality

- Exceptional technology available
- Trust is not binary (Good/Bad)
- We get smarter over time
- Static targets fall
- Government relies on commercial devices
- Government can't control the design
- Shared risk environment

Asymmetric Advantage

PRIVATE SECTOR

Owns and operates

Visibility into systems and networks

Brings expertise and resources



GOVERNMENT

Uniquely sees some threats

Brings elements of national power when necessary

Where Is Cybersecurity Going?



INCORPORATE INNOVATIVE TECHNOLOGY
in cyber defense



INFORMATION SHARING
merges analytics and the knowledge behind it



COLLOBRATE
with partners to effectively counter the adversary


QUESTIONS?