Integrated Cyber Defense for the US Federal Government

Chris Townsend
Vice President, Federal, Symantec

CONSIDER: CHALLENGE / RESPONSE

CLUB	→	SHIELD
SWORD	→	ARMOR
HIGH WALLS	→	TREBUCHET
GUNS	→	TANKS
HIGH GROUND	→	AIR STRIKES
RADAR	→	SATELLITE COMM

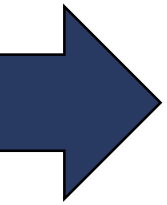
WHAT ABOUT NOW?

SPACE

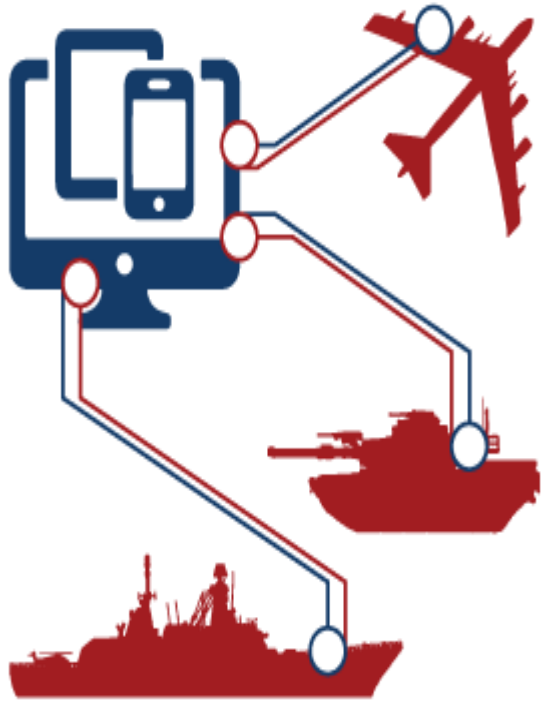
AIR

WATER

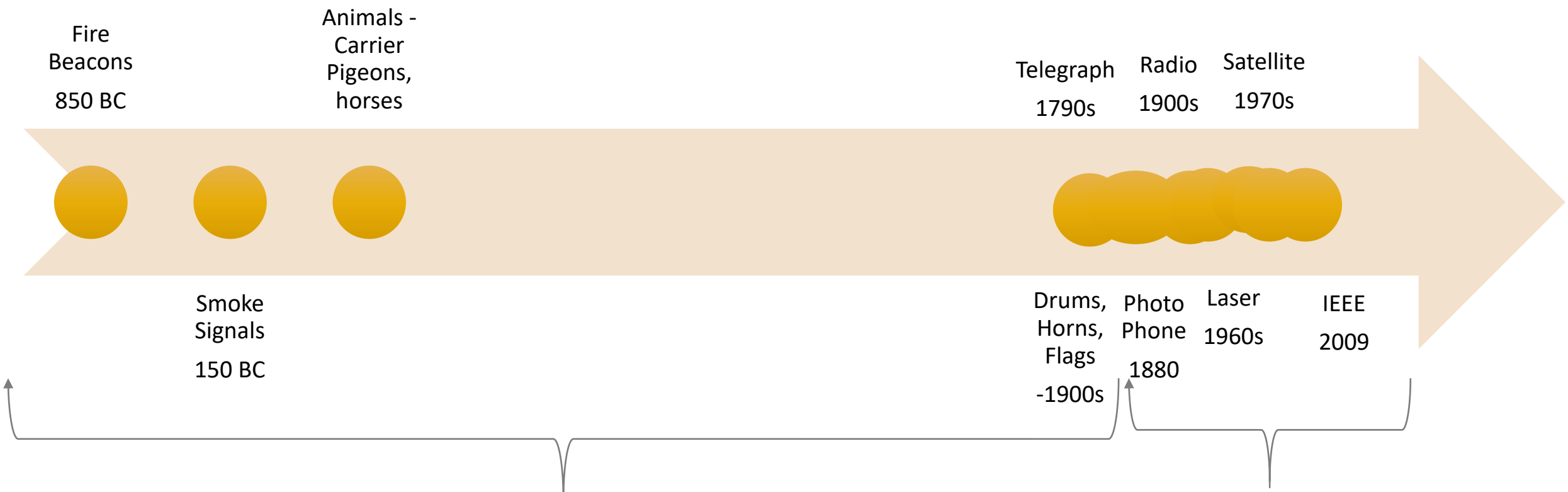
GROUND



COORDINATED COMMAND & CONTROL



Timeline of Military Communications



BUT…
HOW ABOUT CYBER?

There are MILLIONS of Threats & Attack Vectors

Symantec

State-Sponsored Attacks

TDK

LIVING OFF THE LAND

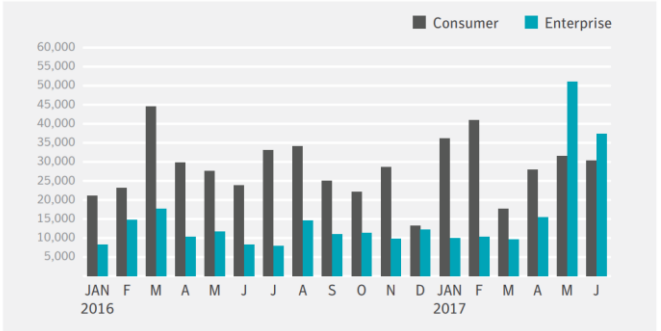
Exploit in memory e.g. SMB EternalBlue	**Non-persistent**	Dual-use tools e.g. netsh PsExec.exe
Email with Non-PE file e.g. Document macro	Memory only malware e.g. SQL slammer	Memory only payload e.g. Mirai DDoS
Remote script dropper e.g. LNK with Powershell from cloud storage	**Persistent**	Non-PE file payload e.g. PowerShell script
Weak or stolen credentials e.g. RDP password guess	Fileless persistence Loadpoint e.g. JScript in registry	Regular non-fileless payload
	Regular non-fileless method	

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

Malware?

RANSOMWARE

Consumer vs enterprise ransomware infections, 2017 to date



Organized Bad Actors?

dragonfly, 2.0

AND HOW DO WE RESPOND? WITH DISPARATE TOOLS & VENDORS

Malwarebytes
Symantec
Lumension IT Secured. Success Optimized.
Symantec
McAfee
Microsoft
tripwire
VARONIS
Ping Identity
okta
RSA
gemalto security to be free
Fidelis
TANIUM
BlackBerry
Good Powered By BlackBerry
McAfee
ca technologies
Symantec
RSA
McAfee
GlobalSign GMO Internet Group
Symantec
zscaler
Symantec
BRADFORD NETWORKS
Hewlett Packard Enterprise
iMPERVA
MetaMatrix
FireEye
RSA Archer GRC
evident.io
Symantec
RISKIQ
BITSIGHT

Email Encryption	Web Proxy
Endpoint Security	URL / Web Filtering
Endpoint Encryption	Email Security
Data Audit	IPS /IDS
Tokens / MFA	Endpoint Mgmt
Forensic	k Mgmt
Mobile S	og Mgmt
DL	vall
Server S	Control
Managed PKI	SSL Decryption
IoT & Guest Access	VA/PT
Database Security	Cloud CASB
Sandboxing	Monitoring & Managed Services
Governance, Risk & Compliance	Business Process Automation

Symantec
Symantec
FORCEPOINT
Symantec
Symantec
Symantec
McAfee
Trustwave
cisco
Check Point
TREND MICRO TippingPoint
Microsoft
redhat
casper SUITE
solarwinds
cisco
FORTINET
TANIUM
splunk
McAfee
exabeam
IMPERVA
cisco
FORTINET
paloalto NETWORKS
ForeScout
ArcSight
Symantec
f5
tenable
WhiteHat SECURITY
skyhigh
Microsoft
QUALYS
SecureWorks
Akamai
ARBOR NETWORKS The Security Division of NETSCOUT
Microsoft
FIREMON
servicenow

Are these the Top DoD Cyber Challenges?

- Defend DoD Networks, Systems and Information
- Defend the United States and its Interests Against Cyber Attacks
- Provide Integrated Cyber Capabilities in Support of Military Operations
- Cyber Security as an Enabler

NO!!! THESE ARE THE <u>OUTCOMES</u> WE ARE TRYING TO ACHIEVE.

Our Challenges are Internal

- Lack of Standards/Integration/Automation
- Limited Human Capital/Cyber workforce
- Lack of good metrics – efficacy/ROI
- Alignment to Cyber Plan/Architecture
- Align to risk mitigation plan
- Procurement - LPTA
- Collaboration/communication
- Limited Resources/Budget

"Complexity is the Enemy of Security"

Howard Schmidt
Gartner Security & Risk Conference Key Note
June 2012

Are COTS Tools the Best Option?

Or Should Cyber Defenses be Purpose Built?

THE ANSWER TO ME IS CLEAR…

It is Time for a Cyber Security Manhattan Project

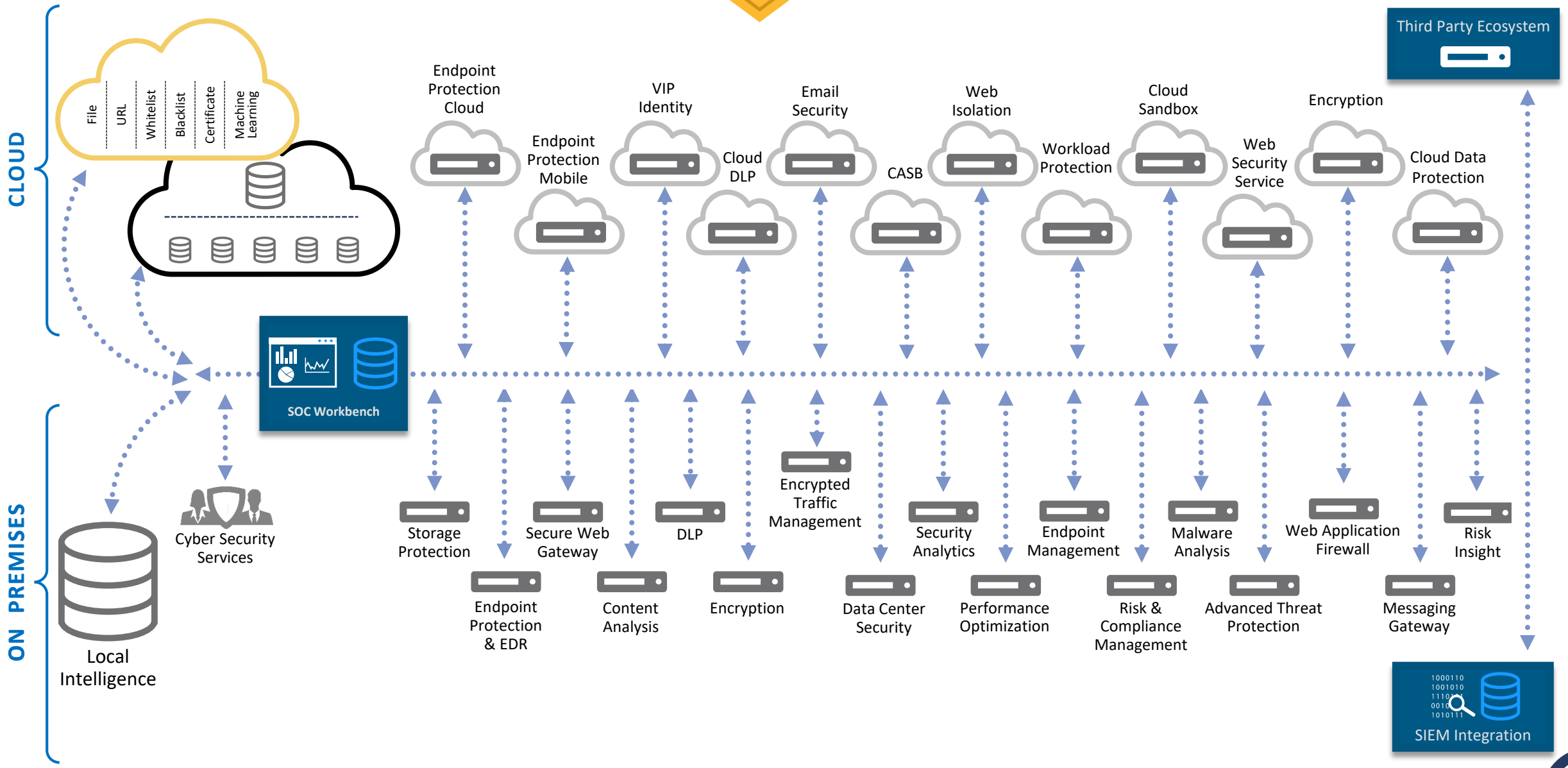
Symantec

THE HILL

Time for the US to develop a Manhattan Project in Cybersecurity
BY GREG CLARK, OPINION CONTRIBUTOR — 09/20/17 06:40 AM EDT

http://thehill.com/opinion/cybersecurity/351387-time-for-the-us-to-develop-a-manhattan-project-in-cybersecurity

Integrated Cyber Defense Platform



OUR ACTION – THE TAKEAWAYS

1. Plan – We Need an Architecture That Makes Sense!

2. Collaborate – Force the Issue From the Top Down – and Outside to the SI's, SPS, DIB and Manf/Vendors

3. Push for a "Manhattan Project" type effort - the adversaries are already doing it!

Thank you!

Chris_Townsend@symantec.com