

# CYBERWAR

Sandun Bambarandage  
INTERFACE



# WHAT'S IN A NAME?

- 'Cyber' vs. 'Kinetic'
- Information Warfare
- Cyberattack vs. Cyberwarfare
- Opinion 1 – Cyber actions that cause damage comparable to kinetic warfare
- Opinion 2 – No cyber actions to date count as 'war' (Iran 2010, DPRK 2014)

# THE NEW KID ON THE BLOCK

- Technology
  - (Relatively) low RD&A costs
  - (Relatively) cheaper to acquire/train personnel
- Use
  - Easy force projection
  - Deterrence is complicated
    - Weapon value significantly falls after use
  - Non-state actors are major players
- Attribution is hard

# Information Security IndustryScape

## SECURITY MANAGEMENT AND COMPLIANCE

**Managed Security Service Providers**

IBM, at&t, verizon, Raytheon, hp, NTT, Dell, CSC, BT, Trustwave, CenturyLink, Symantec

**SIEM**

hp, EMC, RSA, McAfee, splunk, TIBCO, BlackStylus, eventTracker, NetIQ, LogRhythm, tenable, Trustwave, solarwinds

**Security Training**

Security Monitor, Popcorn Training, He One, SANS, wambot, SCIPP, AUJAS, KnowBe4, Security Innovation, Safelight, fishnet, junglemep, PHISHME, PhishLine

**Governance, Risk and Compliance**

software, CMO, SAP, IBM, CYBERARK, protiviti, sas, enablon, mega, SAS GLOBAL, RESOLVER, EMC, RSA, MetricStream, WYNDAM

## INFRASTRUCTURE SECURITY

**Data Masking**

IBM, greenleaf, end-tools, informatica, SOLIX, PI-USE, MENTIS, AXIS, Voltage, ORACLE

**Enterprise Network Firewalls**

Hillstone, JUNIPER, CISCO, Fortinet, AhnLab, Check Point, WatchGuard, Palo Alto, McAfee

**Intrusion Prevention Systems**

STONESOFT, IBM, McAfee, NSFOCUS, hp, enterasys, HUAWEI, CISCO, radware, SOURCEfire, CORN SECURITY

**Network Access Control**

ForeScout, Cisco, aruba, portnox, infoexpress, SAUCONET, JUNIPER, IXIA, BRAD FORD NETWORKS, StillSecure

**Unified Threat Management**

Hillstone, Sophos, Fortinet, Check Point, RAPID7, Barracuda, Juniper, WatchGuard, Cisco, Clavister

## CYBER SECURITY

**Secure Web Gateways**

Blue Coat, Zscaler, Sophos, Barracuda, Trustwave, Intel, Cisco, Symantec, Websense, Sangfor, Trend, iboss

**Network Forensics**

IBM, EMC, RSA, Blue Coat, WildPackets, NARUS, Riverbed, Netscout, NOVETTA, Greenlight, COGNATE

**Threat Intelligence Services**

NORSE, FOX IT, TEAM Cymru, Symantec, trend, SecureWorks, THREATSTREAM, Check Point, LogShoDash, Malwarebytes, JID, Cyveillance, Serice, COGNATE, Digital Smokey, Booz Allen, CIS, IBM, FireEye, One World, Group, CODENOMICON, VeriSign, Securonix, Webroot

## ENDPOINT SECURITY

**Secure Email Gateways**

SOPHOS, Barracuda, Websense, Cisco, WatchGuard, Mimecast, Fortinet, Microsoft, Symantec, SilverSky

**Data Loss Prevention**

Absolute Software, Websense, Vormetric, Trustwave, Symantec, Zecurion

**Endpoint Protection & Anti-virus**

IBM, Sophos, Panda, F-Secure, Check Point, Microsoft, Symantec, Bird defender, McAfee, Eset, LANDesk

**Endpoint Threat Detection & Response**

Avast, Zonefox, Trend, Dtex, LogRhythm, CounterBack, Tanium, Invincea, Nextthink, Cybereason, Cylance, Bit9, Bromium, Ziften

## APPLICATION SECURITY

**Application Security Testing**

Quotum, Veracode, HP, Trend, IBM, Coverity, Acunetix, N-Stalker, Pradeo, NT objectives, Appthority

**Web Application Firewalls**

Imperva, Trustwave, DBApp Security, SH-PE, Barracuda, Penta Security, Denyall, ADNovum, Fortinet, Akamai, NSFOCUS, Radware

**Application Control**

Lumension, McAfee, Faronics, Ditz, Varianity, Trend, Arellia, Kaspersky

## CLOUD SECURITY

Blue Coat, Sophos, CloudLock, Zscaler, Websense, Skyhigh, CloudPassage, ARMOR, SafeNet, McAfee, Bitdefender, Symantec, Trend, Cisco

## MOBILE SECURITY

**Mobile Data Protection**

Dell, Intel, CenterTools, Symantec, Microsoft, Wipac, Trend, Digital Guardian, Wave, Sophos, Kaspersky, Check Point

**Mobile Device Management**

SAP, SOTI, Absolute Software, Citrix, Good, IBM, Airwatch, Symantec, Tangoe, Mocana

## IDENTITY AND ACCESS MANAGEMENT

**User Authentication**

HID, EMC, RSA, Entrust, Equifax, gemalto, DEEPNET SECURITY, mi-token, VASCO, TeleSign, SecuRing, Microsoft, SWIVEL, Symantec, SECUREAUTH, AUTHENTIFY, Duo, SafeNet, OnePasscode

**Identity Governance and Administration**

SAP, EVIDENT, Omada, onelogin, caradigm, SailPoint, CA, IBM, COURION, FISCHER, simeio, AlertEnterprise, Hitachi ID Systems, CrossIdeas, AtoS, Aveksa, okta, Deep, Oracle, symplified, covisint, NetIQ, Centrify, betasystems, EXOSTAR, Pingidentity

## SECURITY PARTNERS

UNISYS, fishnet, nexum, AtoS, AccessIT, GuidePoint, ACCUANT, THUNDERCAT, FUJITSU, cadre, BT, dimension data, FORSYTH, NTT, CATHAM, DENIM GROUP

## SECURITY ORGANIZATIONS

**Education & Academic**

Security, IANS, ISIR, QUASP, Mississippi State, CSA, UTSA, CIAC, UMUC

**Professional Associations & Certification**

(ISC)², GIAC, CompTIA, EC-Council, ISACA, FINANCIAL SERVICES, SANS, PCV, IANS, ISSA, TACR, QUASP

**Government**

CESC, NIST, US-CERT, EUR-POL

## SECURITY CONFERENCES

Gartner, Blackhat, RSA, Infosecurity, TEN

## ANALYST HOUSES

ISI Research, Gartner, quocirca, Ovum, ESG, IDC, FORRESTER





L33T H@CKERZ



# WEAPONS OF WAR

- What does a cyberweapon look like?
- Vulnerability, Exploit, Payload
- Holy Grail: 0-days
- Many, many publicly available tools...
- State/Agency owned software (Ghidra etc.)

# THE ART OF WAR

- Stuxnet
- Mirai Botnet
  - Logged onto vulnerable IoT devices with default credentials
  - DDoS attacks on Dyn – DNS service provider
  - Netflix, Github, Reddit, Xbox Live down
- NotPetya
- Olympic Destroyer



# INTELLIGENT SHIPS: THE FUTURE OF NAVAL WARFARE

THE UK'S 'INTELLIGENT SHIP – THE NEXT GENERATION' COMPETITION  
OFFERS A GLIMPSE INTO THE FUTURE OF THE ROYAL NAVY

DSEI PREVIEW: THE TECH AND TOPICS  
WE EXPECT TO SEE THIS YEAR

A YEAR IN CYBERSECURITY WITH THE UK  
NATIONAL CYBER SECURITY CENTRE

MANAGING BIG DATA FOR BETTER  
DEFENCE AND INTELLIGENCE COMMS





F-16 Block 30



F/A-18F Super Hornet



F-35 Lightning

# THE RULES OF WAR

- Government agencies and vulnerabilities
  - Classified as weapons, prevent disclosure?
- Build separate Internets?
- Counter cyberattacks with conventional weapons?
- ‘Geneva Convention’ for cyberwarfare?



