CRICOS: 00233E | TEQSA: PRV12076

GRIFFITH UNIVERSITY

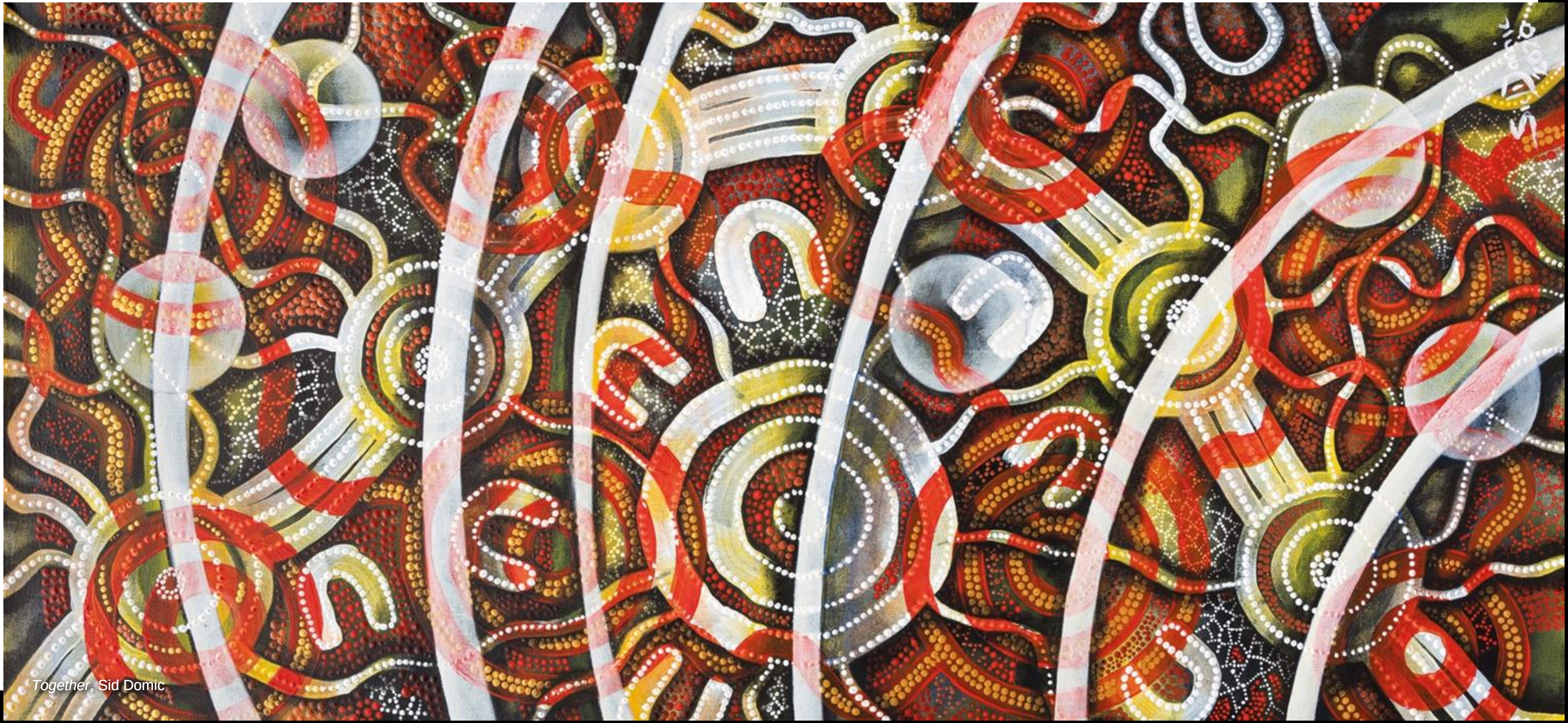
CYBER VULNERABILITIES AND TECHNICAL REGULATION OF CHINA-MADE CCTV IOT SURVEILLANCE CAMERAS IN AUSTRALIA

Ausma Bernot, M. Arif Khan,
Khurram Shahzad, Mart Karakaya,
Conor Healy

IPVM

ACKNOWLEDGEMENT OF COUNTRY

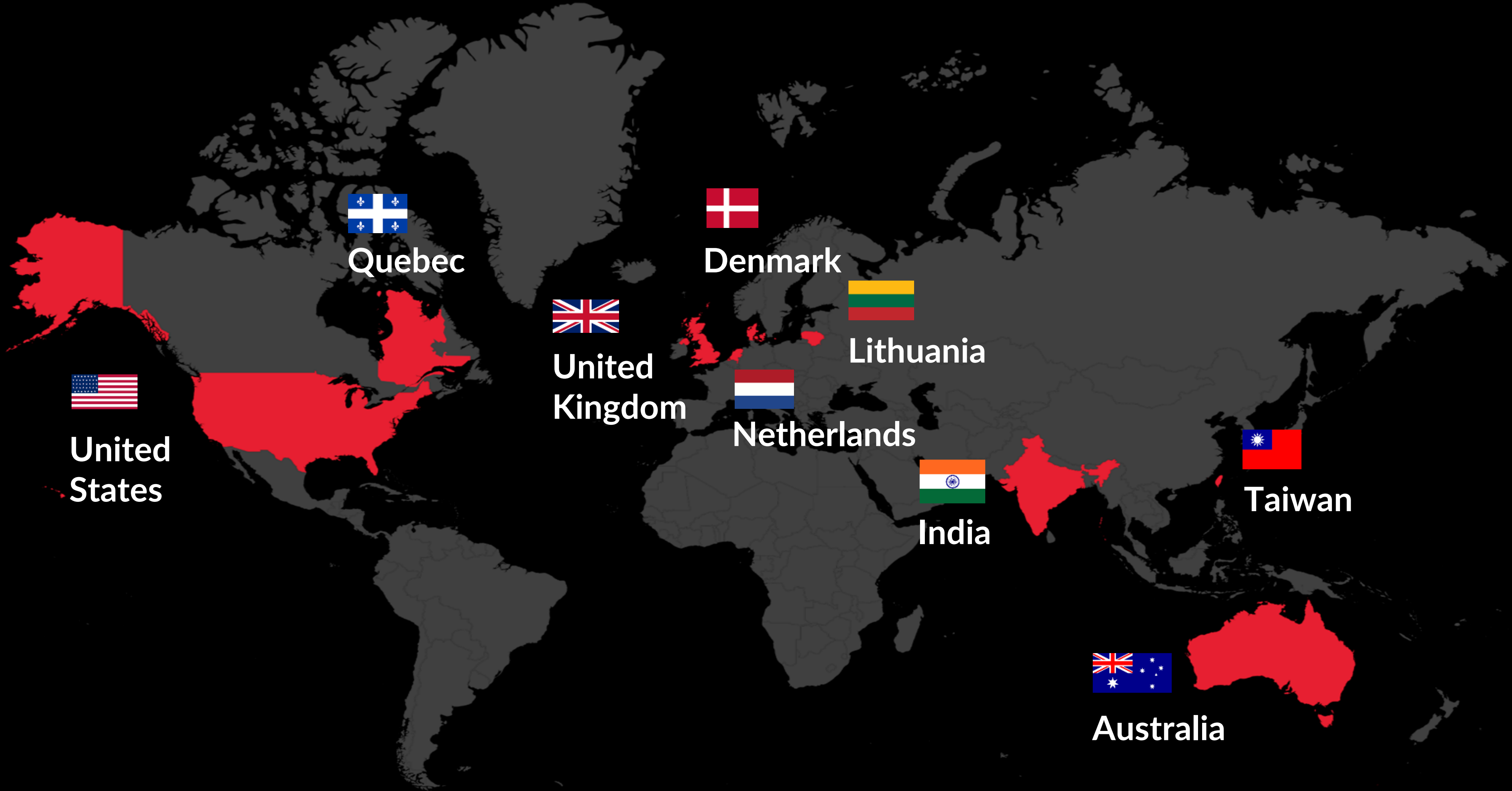
Griffith University acknowledges the people who are the Traditional Custodians of the land. We pay respect to the Elders, past and present, and extend that respect to all Aboriginal and Torres Strait Islander peoples.



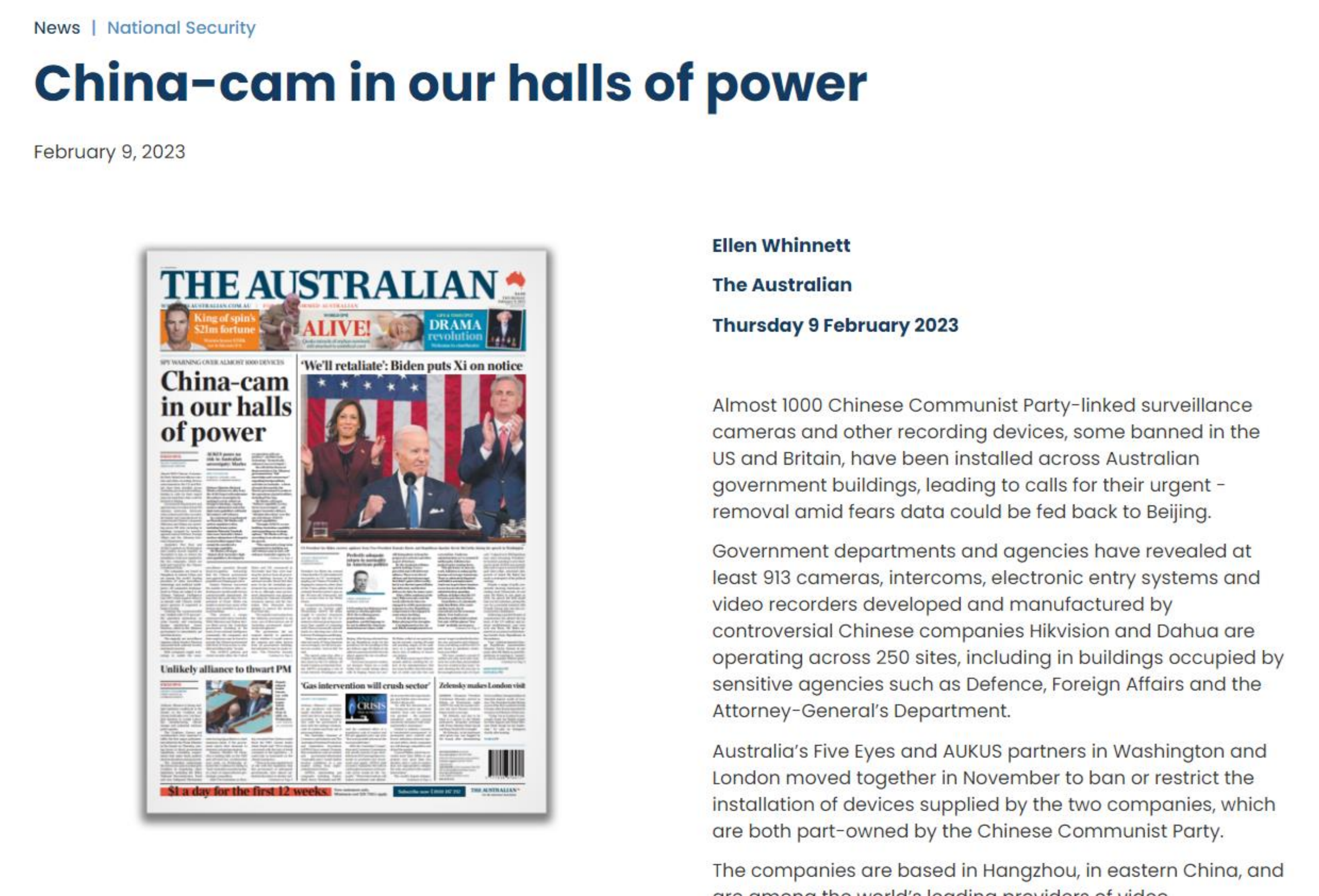
Together, Sid Domic

CRICOS: 00233E | TEQSA: PRV12076

alhua and HIKVISION Restrictions Globally



Research background


THE AUSTRALIAN
'We'll retaliate': Biden puts Xi on notice
Unlikely alliance to thwart PM
'Gas intervention will crush sector'
Zelensky makes London visit
$1 a day for the first 12 weeks

News | National Security

China-cam in our halls of power

February 9, 2023

Ellen Whinnett

The Australian

Thursday 9 February 2023

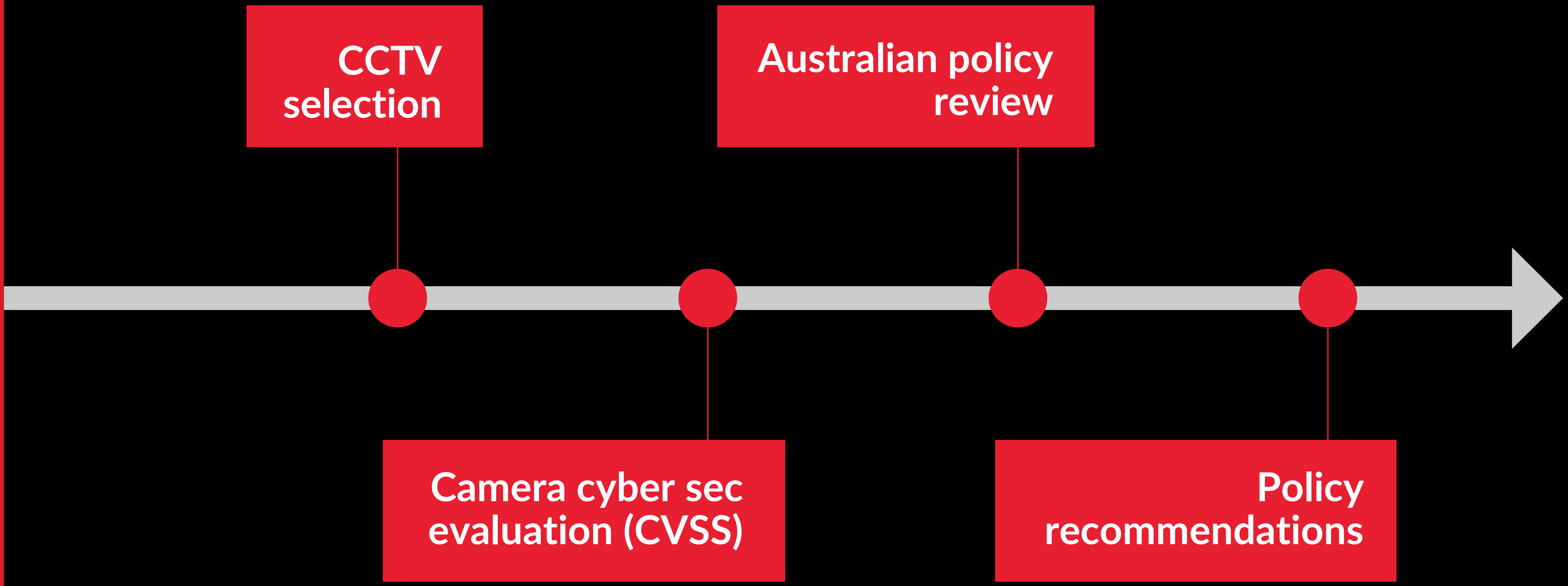
Almost 1000 Chinese Communist Party-linked surveillance cameras and other recording devices, some banned in the US and Britain, have been installed across Australian government buildings, leading to calls for their urgent - removal amid fears data could be fed back to Beijing.

Government departments and agencies have revealed at least 913 cameras, intercoms, electronic entry systems and video recorders developed and manufactured by controversial Chinese companies Hikvision and Dahua are operating across 250 sites, including in buildings occupied by sensitive agencies such as Defence, Foreign Affairs and the Attorney-General's Department.

Australia's Five Eyes and AUKUS partners in Washington and London moved together in November to ban or restrict the installation of devices supplied by the two companies, which are both part-owned by the Chinese Communist Party.

The companies are based in Hangzhou, in eastern China, and are among the world's leading providers of video

Methods



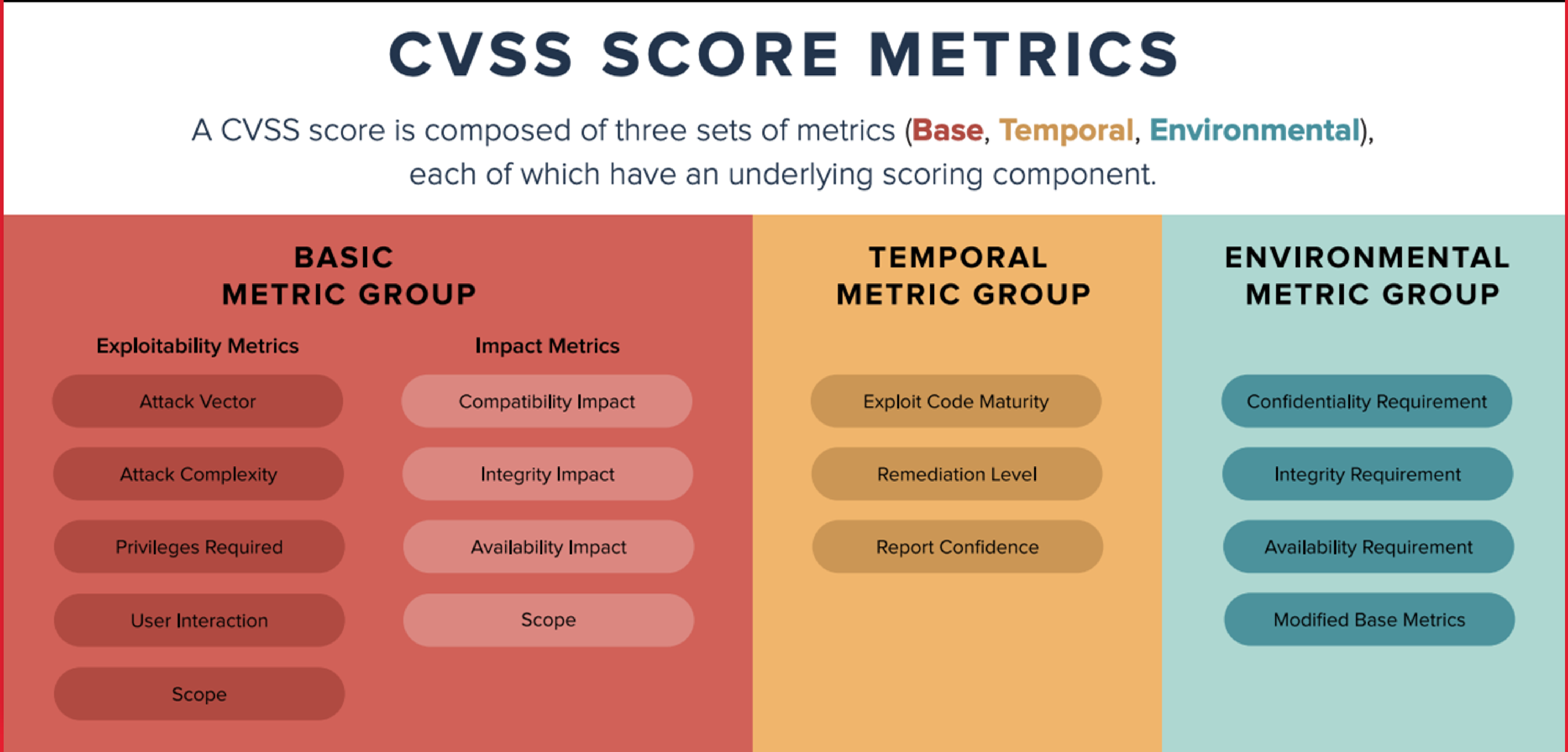
CCTV selection

Camera cyber sec evaluation (CVSS)

Australian policy review

Policy recommendations

CVSS (Common Vulnerability Scoring System)



CVSS SCORE METRICS

A CVSS score is composed of three sets of metrics (**Base**, **Temporal**, **Environmental**), each of which have an underlying scoring component.

BASIC METRIC GROUP

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact Metrics

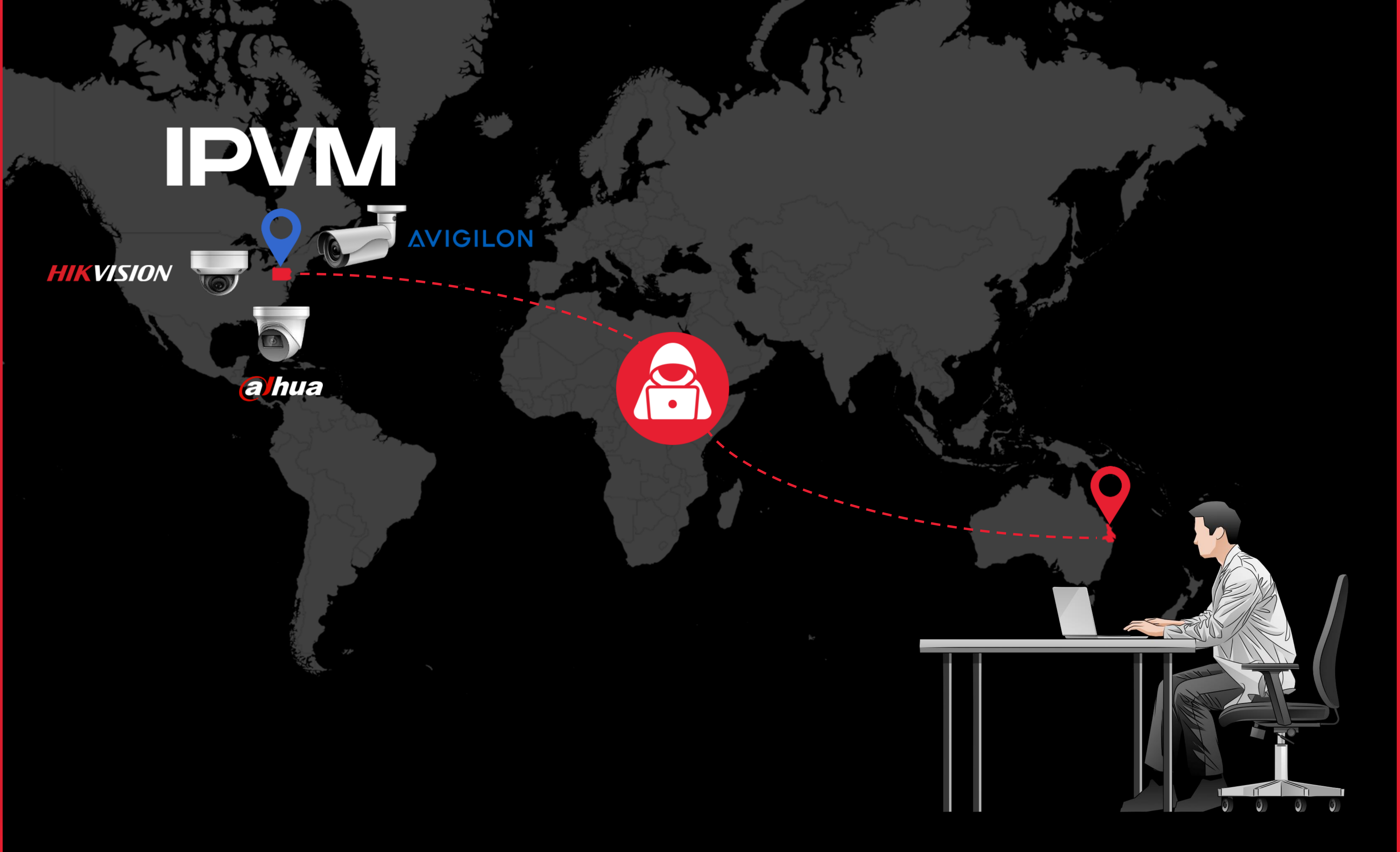
- Compatibility Impact
- Integrity Impact
- Availability Impact
- Scope

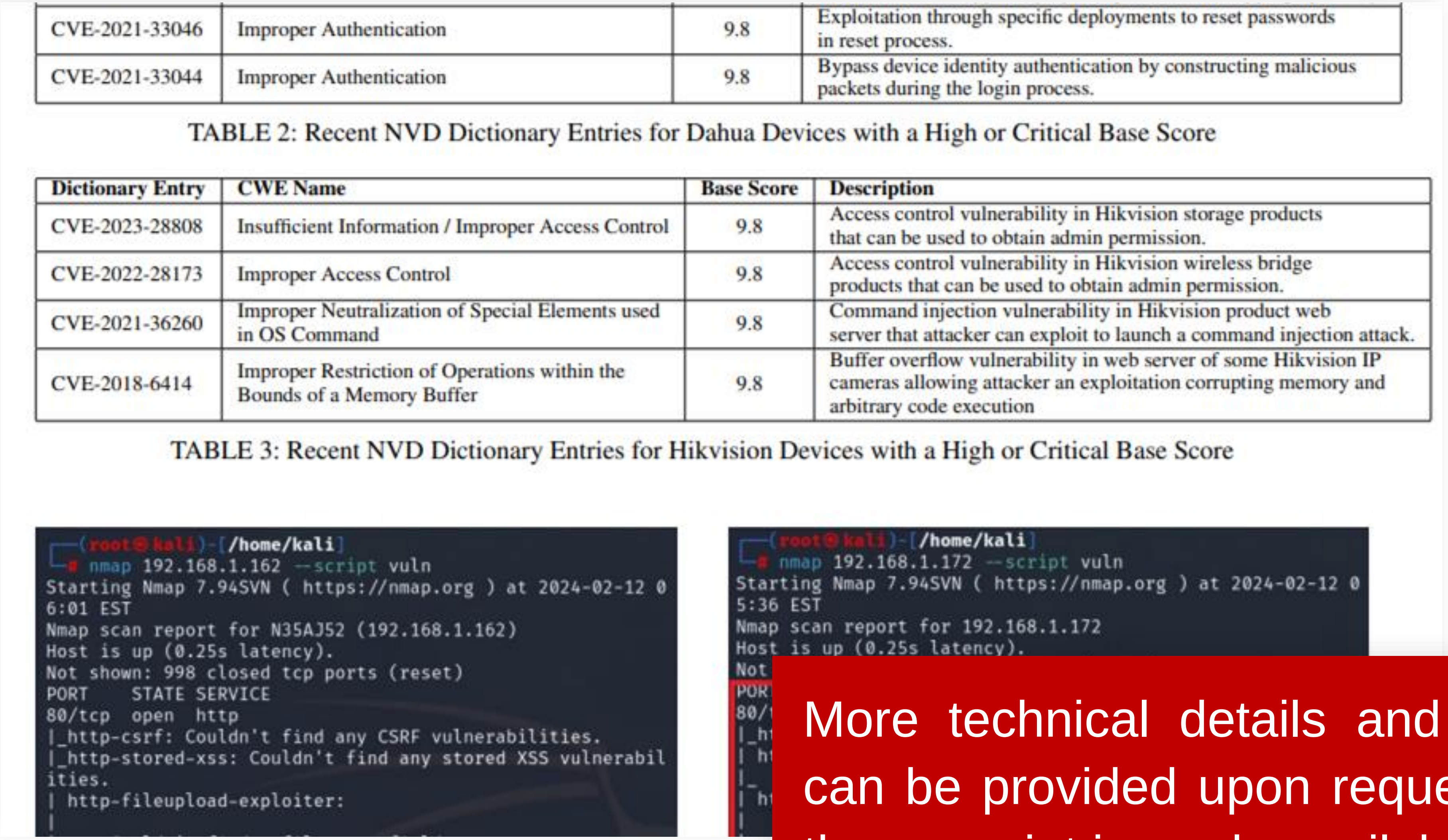
TEMPORAL METRIC GROUP

- Exploit Code Maturity
- Remediation Level
- Report Confidence

ENVIRONMENTAL METRIC GROUP

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics


IPVM
AVIGILON
HIKVISION
alhua



CVE-2021-33046	Improper Authentication	9.8	Exploitation through specific deployments to reset passwords in reset process.
CVE-2021-33044	Improper Authentication	9.8	Bypass device identity authentication by constructing malicious packets during the login process.

TABLE 2: Recent NVD Dictionary Entries for Dahua Devices with a High or Critical Base Score

Dictionary Entry	CWE Name	Base Score	Description
CVE-2023-28808	Insufficient Information / Improper Access Control	9.8	Access control vulnerability in Hikvision storage products that can be used to obtain admin permission.
CVE-2022-28173	Improper Access Control	9.8	Access control vulnerability in Hikvision wireless bridge products that can be used to obtain admin permission.
CVE-2021-36260	Improper Neutralization of Special Elements used in OS Command	9.8	Command injection vulnerability in Hikvision product web server that attacker can exploit to launch a command injection attack.
CVE-2018-6414	Improper Restriction of Operations within the Bounds of a Memory Buffer	9.8	Buffer overflow vulnerability in web server of some Hikvision IP cameras allowing attacker an exploitation corrupting memory and arbitrary code execution

TABLE 3: Recent NVD Dictionary Entries for Hikvision Devices with a High or Critical Base Score

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.162 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 0
6:01 EST
Nmap scan report for N35AJ52 (192.168.1.162)
Host is up (0.25s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabil
ities.
| http-fileupload-exploiter:
|
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.172 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 0
5:36 EST
Nmap scan report for 192.168.1.172
Host is up (0.25s latency).
Not
POR
80/
|_h
| h
|_
| h
|
```

More technical details and findings can be provided upon request, once the pre-print is made available.

Policy evaluation: Binding standards

Binding

Standards Australia: General IoT and CCTV regulations

Engineers Australia recommendation to the Australian Government on the '2023-2030 Australian Cyber Security Strategy':

(1) ETSI EN 303 645

(2) IEC 62443

ETSI EN 303 645 supported by the **Office of Impact Analysis** in December 2023

Non-Binding

Information Security Manual (ISM), released December 2023

Australian Security and Intelligence Organisation's **T4 protective security**

The Protective Security Policy Framework (PSPF)

Australian Signals Directorate **13 non-binding security-by-design principles**

Key Findings

Technical

- CVSS: All products contain vulnerabilities, High or Critical base score vulnerabilities only present in Hikvision and Dahua
- Tech governance: History of Hikvision and Dahua governance internationally

Policy

- Policy evaluation: Overlapping cyber hygiene policies
- Technical regulation: Limited, non-binding, not harmonised
- Consumers: Limited information available for consumers

THANK YOU!

Dr Ausma Bernot, Lecturer in Tech and Crime, Griffith University

a.bernot@griffith.edu.au

Conor Healy, Director, Government Research, IPVM

chealy@ipvm.com