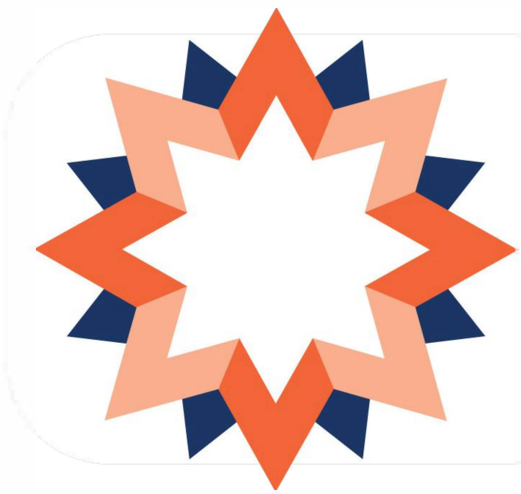
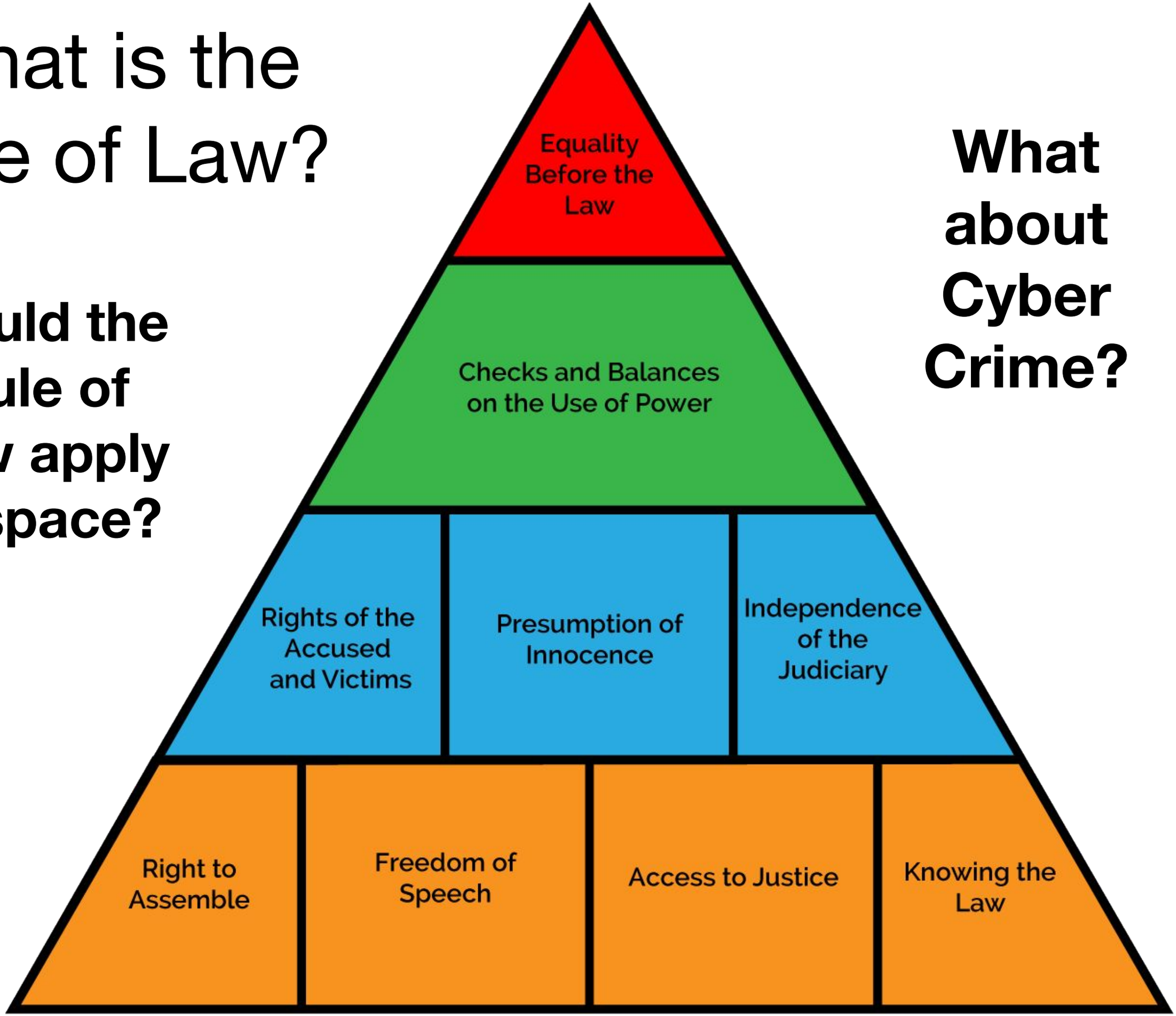
Technology and the Law



RULE OF LAW
INSTITUTE OF AUSTRALIA

What is the Rule of Law?

Would the Rule of Law apply in space?



What about Cyber Crime?

Space law 'groaning with age' as race to commercialise the cosmos takes off

RN By Erica Vowles for The Law Report

Updated about 5 hours ago

In January, United States company Swarm Technology succeeded in launching their prototype satellites — each smaller than a loaf of bread — into orbit.

With hundreds of satellites launched every year, Swarm's success would have been otherwise unremarkable, except for one fact: they had been denied launch approval by US authorities.

The company went ahead anyway.

Professor Melissa de Zwart, the dean of law at Adelaide University Law School, said Swarm took

PHOTO: As more private companies launch into space, the

Outer Space Treaty 1967

Australia & US sign Space Tracking Treaty

By **Deyana Goh** - October 19, 2017

Image of the Canberra Deep Space Communication Complex , courtesy of NASA.

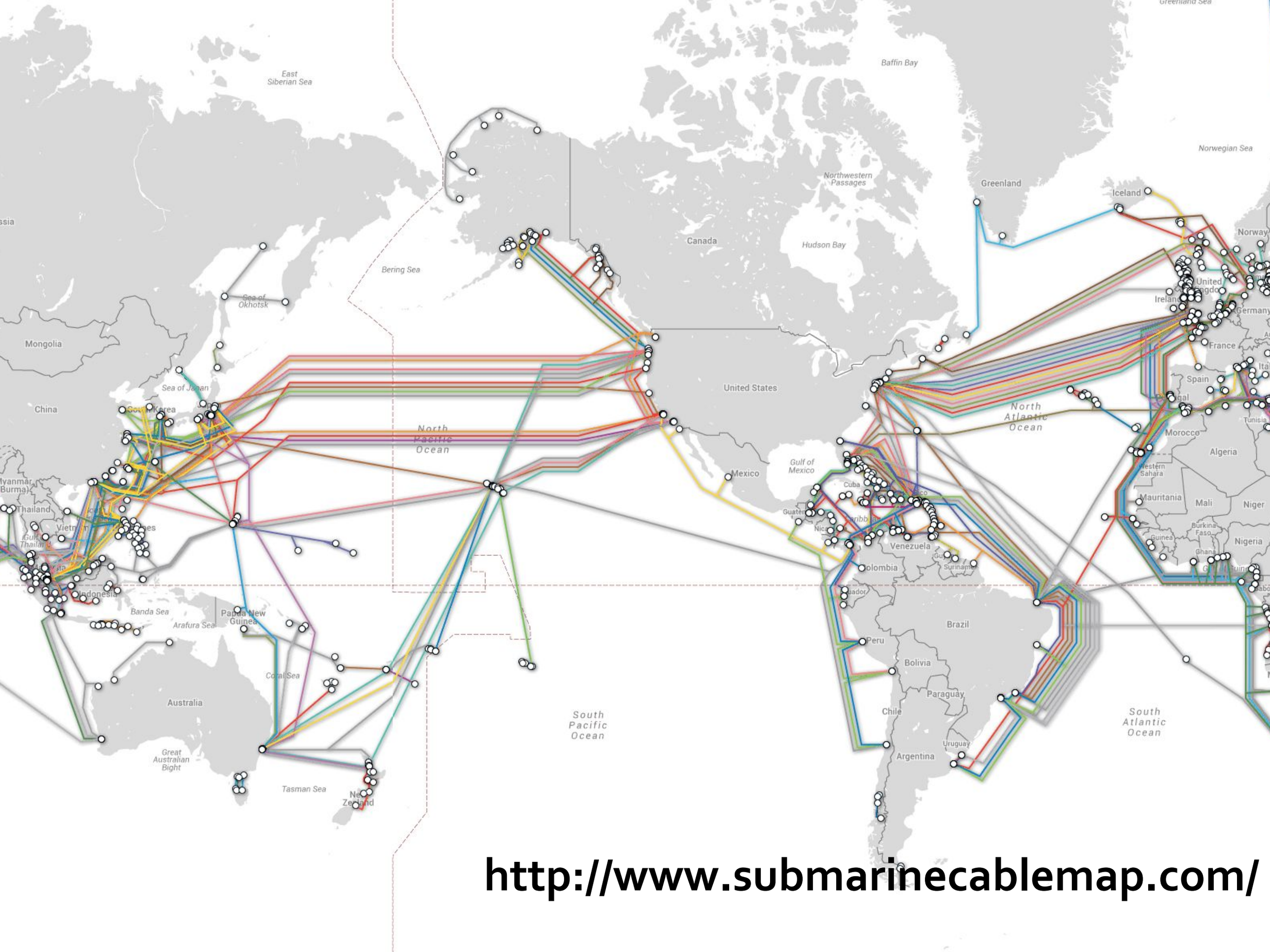
Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies

Space Activities Amendment (Launches and Returns) Bill 2018

- Law reform
- Reasons for change:
- operating environment continues to change.
- type of activities being undertaken and the new participants involved: businesses and universities.
- the Act has predominantly supported the space industry to launch satellites from overseas, where an Australian national is a responsible party but this needs to change.
- The Bill: broadens the regulatory framework to include arrangements for launches from aircraft in flight and launches of high power rockets; and reduces barriers to participation in the space industry, by streamlining approval processes and insurance requirements for launches and returns

Cyber Crime Definition

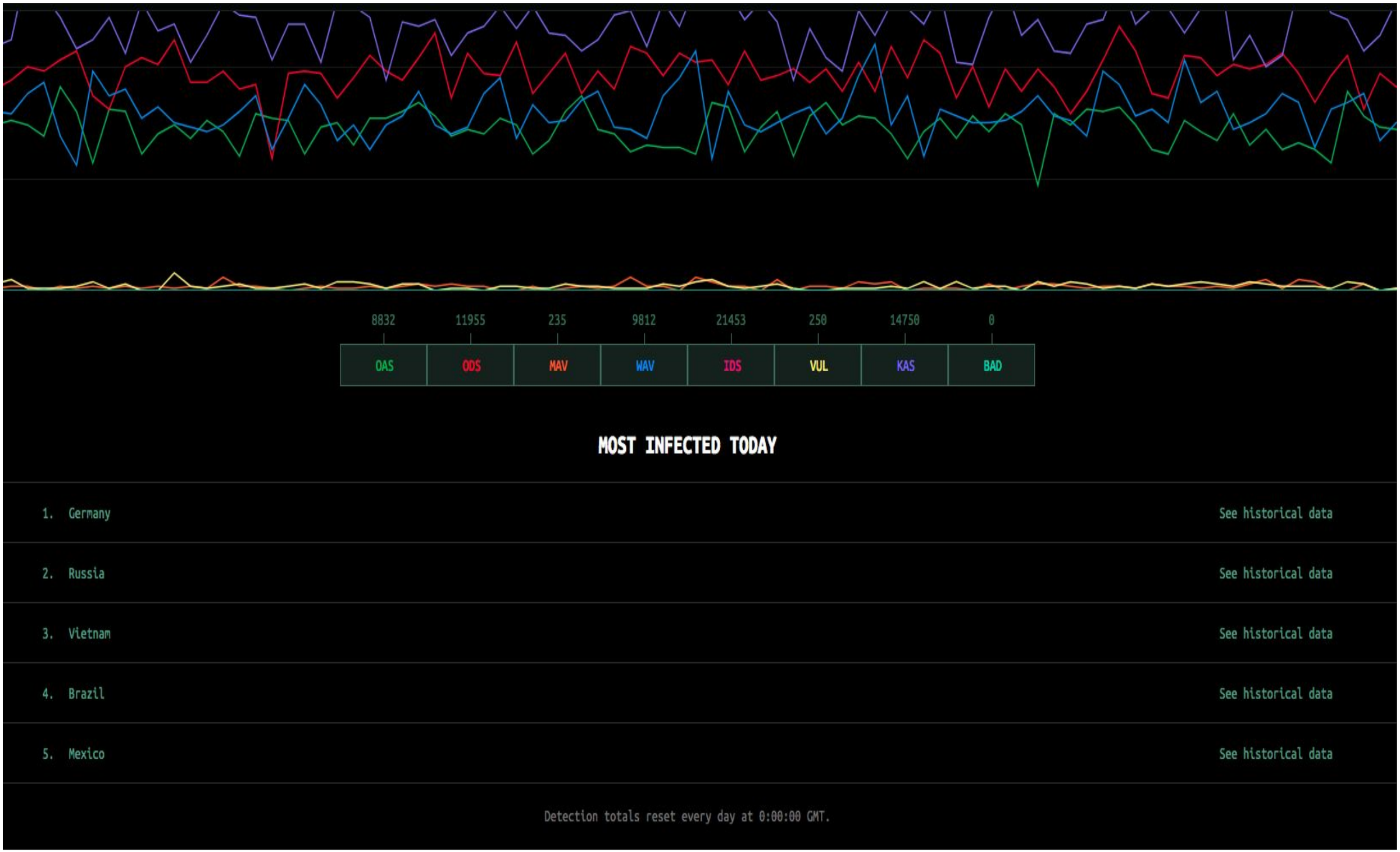
- fraudulent financial transactions
- identity theft
- theft of information for commercial gain/piracy
- drug trafficking
- money laundering
- image based sexual abuse
- harassment, stalking and other threatening behaviours
- terrorist recruitment and propaganda



http://www.submarinecablemap.com/

CLOUD Act

- American law
- Clarifying Lawful Overseas Use of Data Act 2018
- allows: U.S. to enter into bilateral data-access agreements with like-minded countries.
- Foreign law enforcement to pursue data stored in the U.S. through their own legal processes and vice-versa, provided that the country meets the necessary legal and civil liberty requirements outlined in the legislation



20/6/2018

https://cybermap.kaspersky.com/

Bank details, TFNs, personal details of job applicants potentially compromised in major PageUp data breach

By Pat McGrath and Clare Blumer, ABC Investigations

Updated 21 minutes ago

The personal details of thousands of Australians have potentially been compromised, with HR company PageUp, which counts Telstra, NAB, Coles, Australia Post, Aldi and Medibank as clients, revealing a massive data breach.

PageUp, which boasts 2 million active users across 190 countries, posted a statement from chief executive Karen Cariss on its website, saying it had noticed "unusual activity" in its IT infrastructure on May 23.

The company has launched an investigation, while

PHOTO: The personal details of thousands of Australians has potentially been compromised due to a data breach.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

.....@gmail.com pwned?

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

tumblr: In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

Compromised data: Email addresses, Passwords

Data Breach Notification Laws

- Data breach Legislation - **Privacy Amendment (Notifiable Data Breaches) Bill 2016**

- Passed by Parliament 22 February 2017

Amends the **Privacy Act 1988 (Cth)**

"*An eligible data breach happens if:*

(a) there is ***unauthorised access to, unauthorised disclosure*** *of, or loss of,* ***personal information*** *held by an entity; and*

(b) the access, disclosure or loss is likely to ***result in serious harm*** *to any of the individuals to whom the information relates.*

An entity must give a notification"

Page Up Data Breach

Dear Sir/Madam
… this Department has engaged a firm known as PageUp for the provision of online recruitment services for vacancies. You may be aware of recent media reports concerning unauthorised access to PageUp systems, which has involved potential access to, and disclosure of, personal data relating to job applicants.

Although PageUp is continuing to investigate and monitor the impact of this incident, I am writing to notify you that it is possible that some of your personal details which were held in PageUp's systems may have been accessed by an unauthorised person and possibly disclosed to others.

….the following information input onto PageUp forms by applicants seeking employment in this Department may have been obtained by cyber attackers who used advanced methods to gain access to PageUp's IT systems:

- contact details including name, email address, physical address, and telephone numbers;

- biographical details including gender, date of birth (if supplied – AGD does not currently request that applicants provide this information), maiden name (if applicable), nationality, and whether an applicant was a local resident at the time of the application;

- employment details at the time of the application, including employment status, employer details, and title;

- details of nominated referees, including name, contact details and length of relationship with the applicant.

online social

Cyberbullying, revenge porn and sextortion on the rise in Australia, as new laws promise jail time

SEXTORTION, revenge porn, and cyberbullying are on the rise, Australia's online safety agency says, and social networks and parents need to act now.

Jennifer Dudley-Nicholson

News Corp Australia Network MAY 25, 2017 1:15PM

CYBERBULLYING, revenge porn, and sextortion are on the rise and the government agency tasked with fighting the scourge said social networks, parents, and teachers need to do more to stop their spread.

The Office of the Children's eSafety Commissioner today told a Senate Estimates Committee cyberbullying cases soared by 60 per cent over the past year, and warned Australia was "about 10 years behind in terms of education".

Image-based abuse, including revenge porn and sextortion cases, had also risen so rapidly in Australia that the agency planned to drop the word "children" from its title and would invest $4.8 million in an "image-based" reporting tool due to launch later this year.

RELATED: Sexting victim reveals schoolyard hell

RELATED: New revenge porn laws means sharing suacy photos can mean jail

Crimes Amendment (Intimate Images) Act 2017

provides that:

it will be an offence for a person to intentionally record or distribute, or threaten to record or distribute, an intimate image of another person without that person's consent.

The maximum penalty will be imprisonment for 3 years or 100 penalty units, or both.

National Security 1960 to 2016

1960 – Only ASIO could tap phones in relation to matters of national security:

*‘“**the security of the Commonwealth**” means the protection of the Commonwealth and the Territories from acts of espionage, sabotage or subversion, whether directed from, or intended to be committed, within the Commonwealth or not;’*

Telephonic Communications (Interception) Act 1960

1979 – TIA Act, police receive more powers to intercept phone calls in drugs investigations

80s, 90s, 00s – broader powers to access communications, and “stored communications”, and **METADATA.**

2015 – mandatory retention of **METADATA**

2017 - Attorney-General’s Dept. Review calls for submissions on whether **metadata** should be available for use in **civil cases**

What is metadata:

WHO | **WHEN**
WHERE | **HOW**

about a communication.

so you can think about **WHY**:

- Someone is calling someone else?
- they spent 20 minutes on the phone with them at 2 in the morning?
- did they text/sms that person 20 times in one day?
- was that email attachment 20mb?

Mandatory retention of metadata

- Telecommunications companies like Optus, Telstra, iiNet, etc… were **no longer keeping metadata**.

- **Intelligence and law enforcement** agencies pushed for a law that required companies to keep this data for use in investigations.

- Law passed in 2015 requires all telcos to keep **2 years worth of metadata**.

- Intelligence and law enforcement can access this data in **investigations relating to crime or national security**

Does metadata retention work? #effectiveness

- Rick Sarre - Professor of Law and Criminal Justice University of South Australia says:

- **it can be defeated - hence the emphasis on encrypted data…there is no guarantee that it is not being shared internationally…it costs approx $750 million over 10 years…there is little evidence of a causal link to reducing attacks…and it's a threat to privacy**

Key Legislation

- *Crimes Amendment (Intimate Images) Act 2017* (NSW)

- **Data breach Legislation** - *Privacy Amendment (Notifiable Data Breaches) Bill 2016*
  - Amends the ***Privacy Act 1988 (Cth)***

- **Metadata Law:** *Telecommunications (Interception and Access) Act 1979*

- **Recent legislation: Carly's law -** *Criminal Code Amendment (Protecting Minors Online) Act 2017* amends **the TIA act and the Criminal Code Act 1995 (Cth)**

WWW.RULEOFLAW.ORG.AU