Some Legal Aspects of Autonomous Weapons Systems

Sir Richard Williams Foundation Conference

Next Generation Autonomous Systems

8 April 2021

National Gallery of Australia

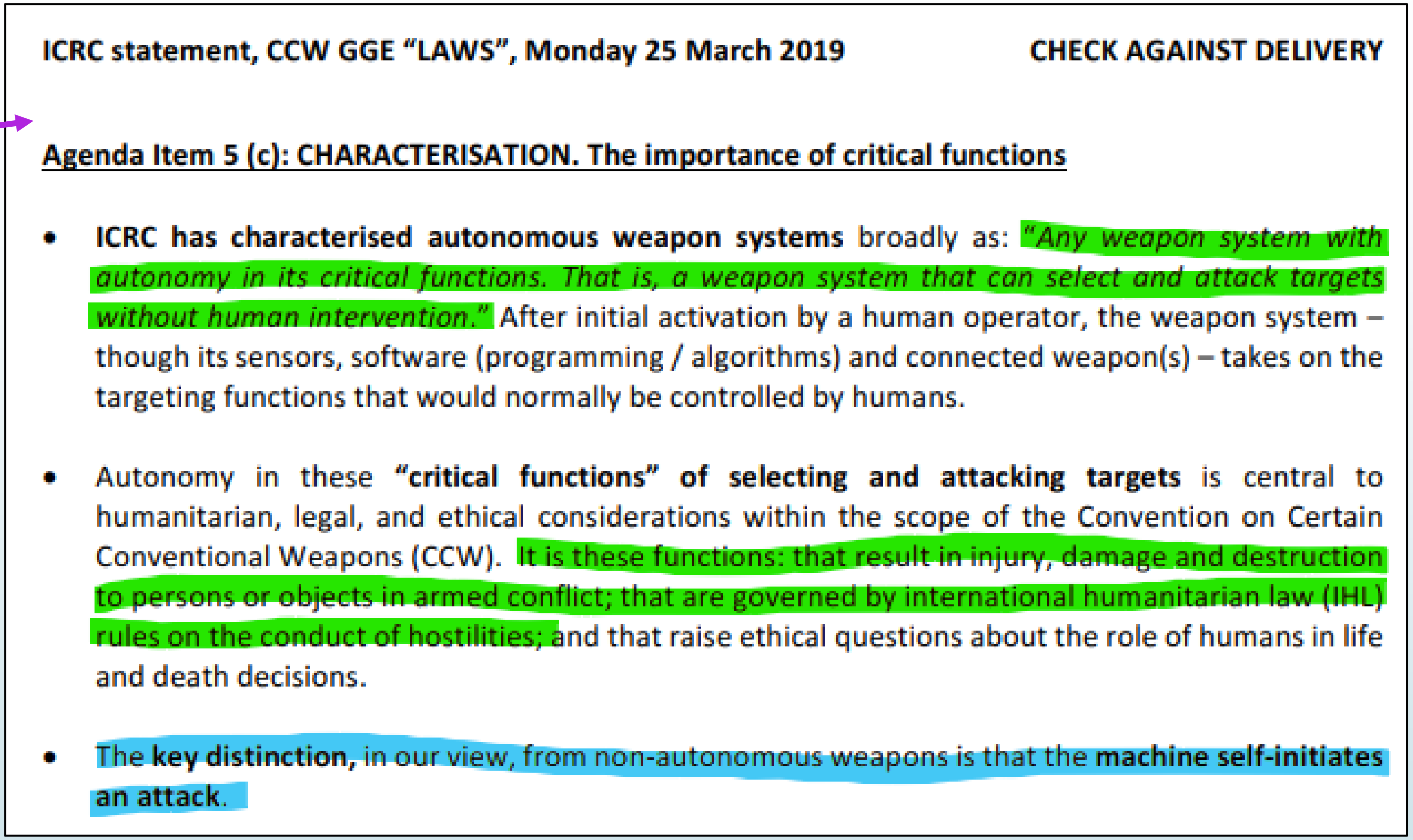
Rob McLaughlin, ANCORS

Outline

- What is an AWS, legally speaking?
    - What challenges do AWS present, legally speaking?
        - An example…
- What is the current state of play in terms of thinking about regulation?
    - Three broad approaches
        - Australian concept of a ‘system of control’
- What risks attend an early an d comprehensive prohibition option?
- Concluding thoughts?

1. What is an ‘autonomous weapon system’?

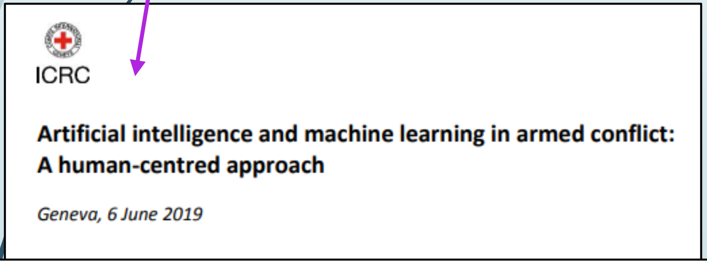
- Many and varied definitions
- A good **definition**, which gets to the nub of many **concerns** about ‘meaningful human control’ over lethal decisions, is that proposed by the International Committee of the Red Cross:



ICRC statement, CCW GGE “LAWS”, Monday 25 March 2019 **CHECK AGAINST DELIVERY**

Agenda Item 5 (c): CHARACTERISATION. The importance of critical functions

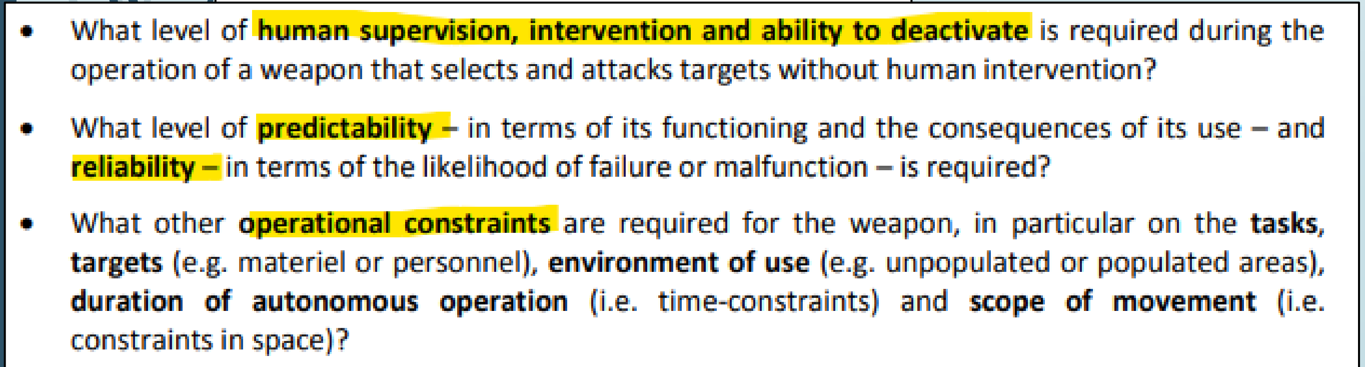
- **ICRC has characterised autonomous weapon systems** broadly as: *“Any weapon system with autonomy in its critical functions. That is, a weapon system that can select and attack targets without human intervention.”* After initial activation by a human operator, the weapon system – though its sensors, software (programming / algorithms) and connected weapon(s) – takes on the targeting functions that would normally be controlled by humans.
- Autonomy in these **“critical functions” of selecting and attacking targets** is central to humanitarian, legal, and ethical considerations within the scope of the Convention on Certain Conventional Weapons (CCW). It is these functions: that result in injury, damage and destruction to persons or objects in armed conflict; that are governed by international humanitarian law (IHL) rules on the conduct of hostilities; and that raise ethical questions about the role of humans in life and death decisions.
- The **key distinction,** in our view, from non-autonomous weapons is that the **machine self-initiates an attack**.



ICRC

Artificial intelligence and machine learning in armed conflict: A human-centred approach

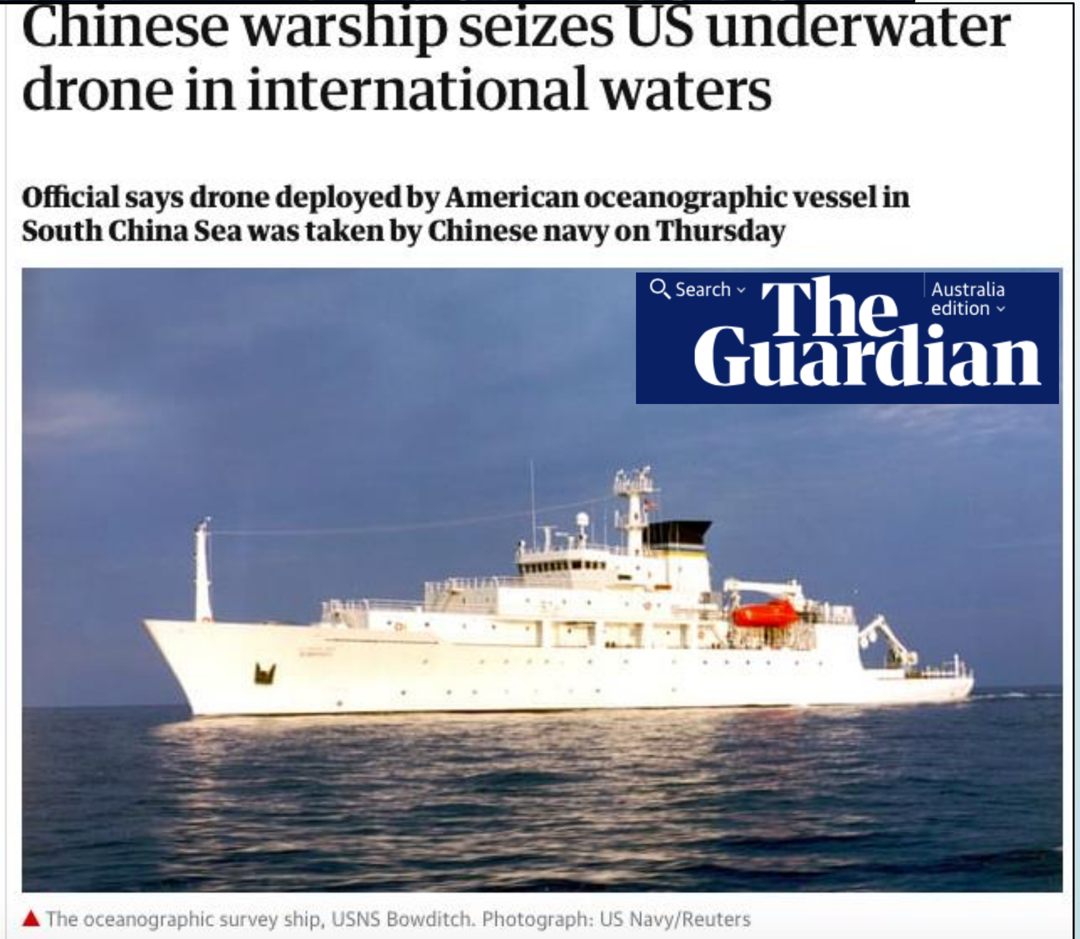
Geneva, 6 June 2019



- What level of **human supervision, intervention and ability to deactivate** is required during the operation of a weapon that selects and attacks targets without human intervention?
- What level of **predictability** – in terms of its functioning and the consequences of its use – and **reliability** – in terms of the likelihood of failure or malfunction – is required?
- What other **operational constraints** are required for the weapon, in particular on the **tasks**, **targets** (e.g. materiel or personnel), **environment of use** (e.g. unpopulated or populated areas), **duration of autonomous operation** (i.e. time-constraints) and **scope of movement** (i.e. constraints in space)?

Size ? System ?

Sovereign immune ‘asset’ ?



Chinese warship seizes US underwater drone in international waters

Official says drone deployed by American oceanographic vessel in South China Sea was taken by Chinese navy on Thursday

▲ The oceanographic survey ship, USNS Bowditch. Photograph: US Navy/Reuters

- When is an AWS a system, or a component of a system?
  - How do we conduct 1977 Additional Protocol I article 36 weapons reviews, and on which ‘bits’?
- When is the AWS (in legal terms) an independent unit (like a warplane or a warship) rather than simply a sensor / weapon?
  - Implications for AWS legal status and the rights (eg navigation) the AWS can exercise under the law of the sea and in airspace?

Example: Can a Maritime Autonomous Weapons System be a ‘Warship’?

- LOSC 1982 definition - Art 29

For the purposes of this Convention, **‘warship’** means a ship belonging to the armed forces of a State bearing the external marks distinguishing such ships of its nationality, **under the command of** an officer duly commissioned by the government of the State and whose name appears in the appropriate service list or its equivalent, and **manned by a crew** which is under regular armed forces discipline.

Bundesarchiv, Bild 146-1985-074-27
Foto: o.Ang. | 1940/1941 ca.

Can a Maritime AWS be an ‘auxiliary’?

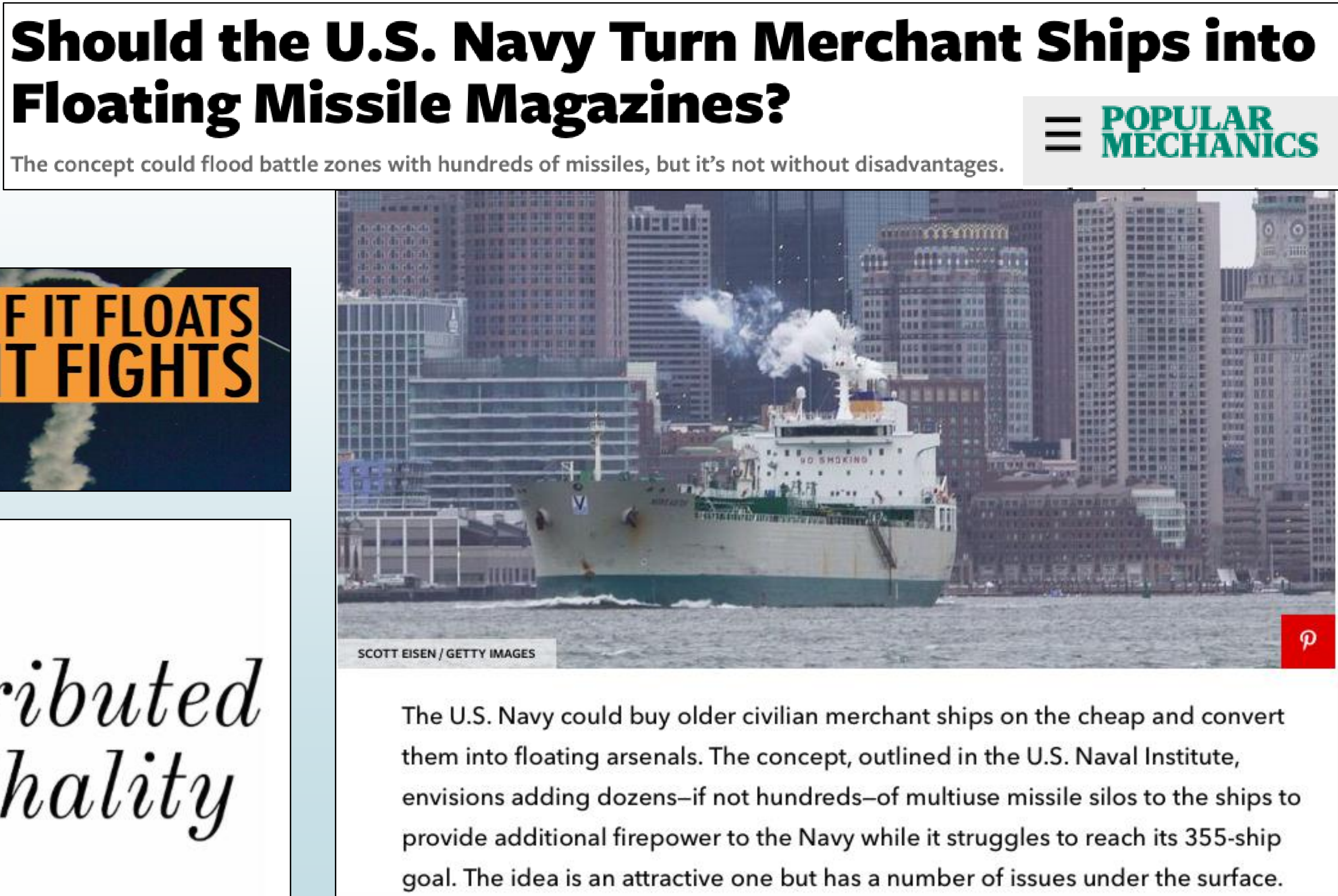
San Remo Manual 1995:

13. For the purposes of this document: …

(h) **auxiliary vessel** means a vessel, other than a warship, that is owned by or under the exclusive control of the armed forces of a State and used for the time being on government non-commercial service…

But auxiliaries do not have ‘belligerent rights’… (self-defence, yes; attack, no)

Lawful ?



Should the U.S. Navy Turn Merchant Ships into Floating Missile Magazines?

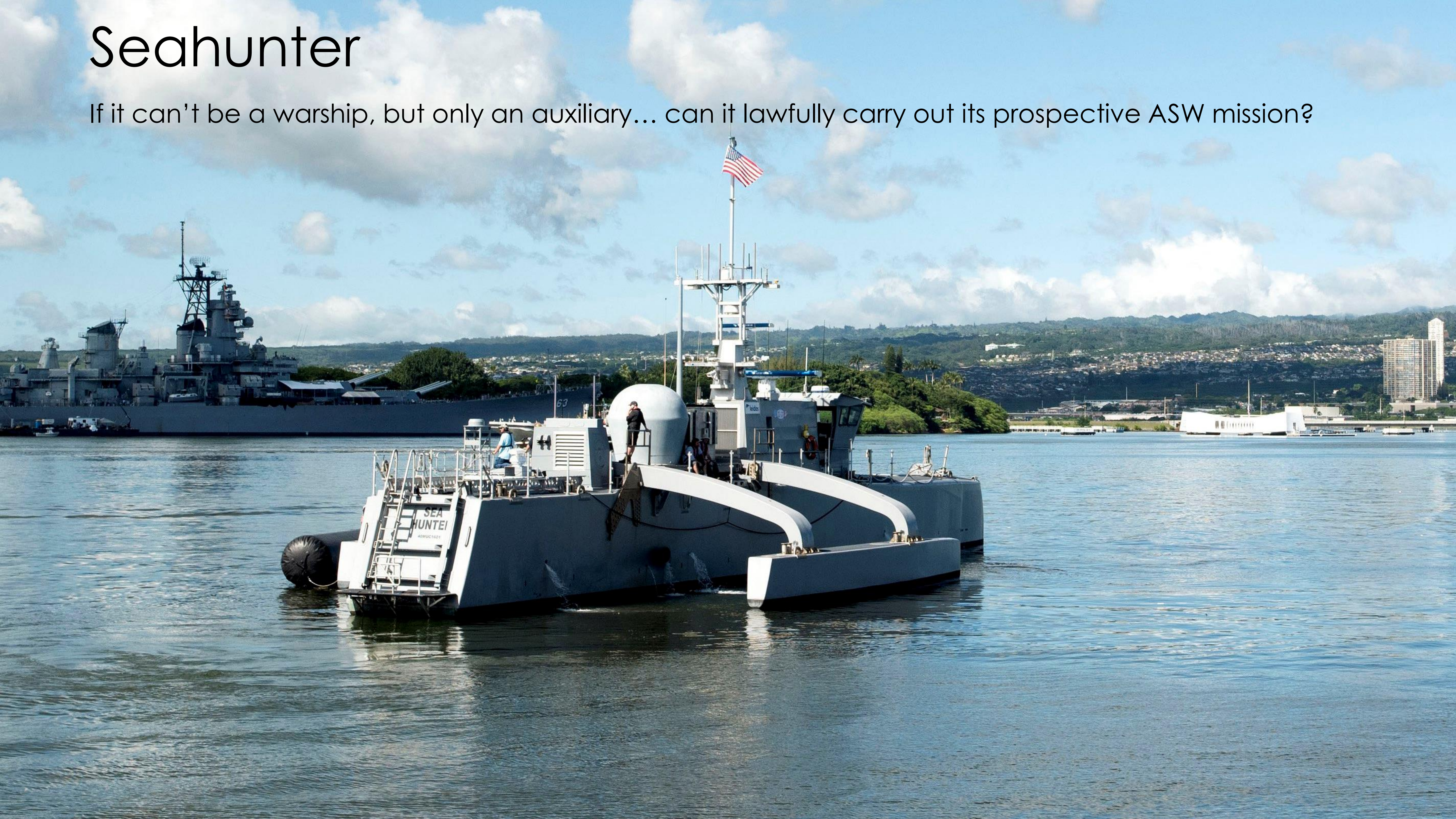
The concept could flood battle zones with hundreds of missiles, but it's not without disadvantages.

SCOTT EISEN / GETTY IMAGES

The U.S. Navy could buy older civilian merchant ships on the cheap and convert them into floating arsenals. The concept, outlined in the U.S. Naval Institute, envisions adding dozens—if not hundreds—of multiuse missile silos to the ships to provide additional firepower to the Navy while it struggles to reach its 355-ship goal. The idea is an attractive one but has a number of issues under the surface.

Seahunter

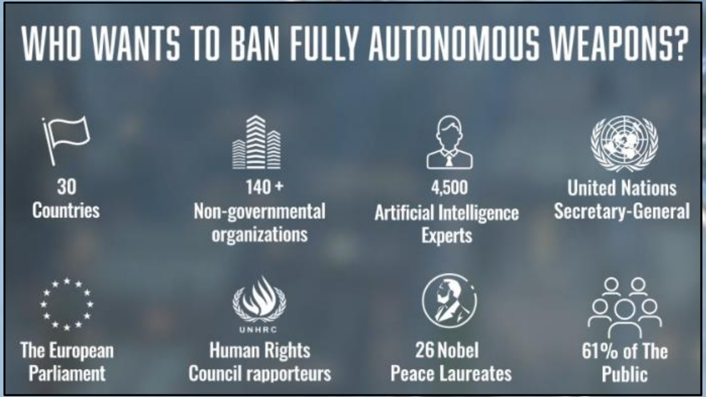
If it can't be a warship, but only an auxiliary… can it lawfully carry out its prospective ASW mission?

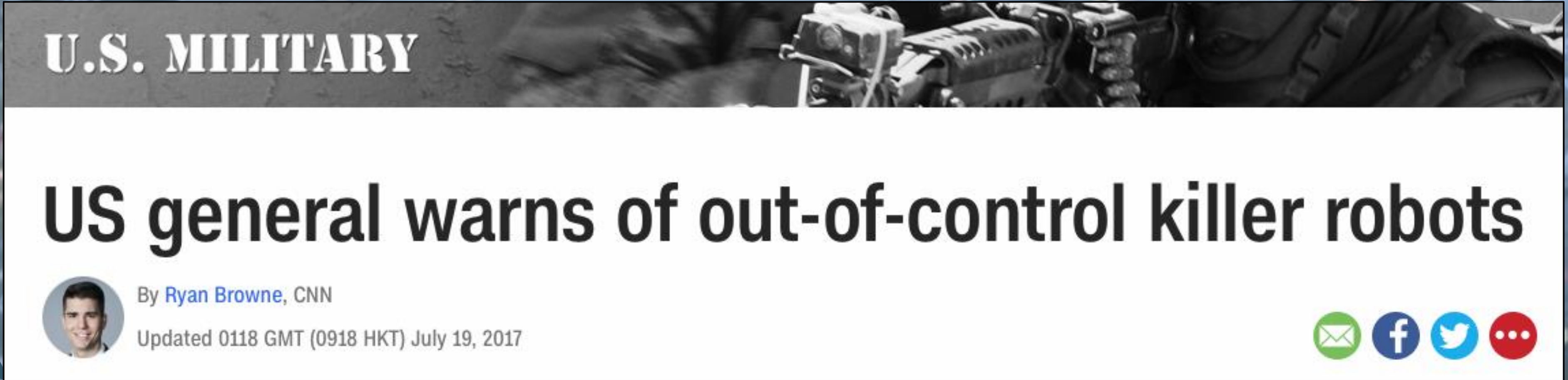


2. Current state of play as regards thinking about regulation of AWS?

- What keeps us up at night? Fully autonomous weapon system in urban environment, lots of civilians and civilian objects, real distinction challenges
- But is this concern driving the debate about a complete prohibition?

CAMPAIGN TO STOP KILLER ROBOTS


WHO WANTS TO BAN FULLY AUTONOMOUS WEAPONS?
30 Countries
140 + Non-governmental organizations
4,500 Artificial Intelligence Experts
United Nations Secretary-General
The European Parliament
UNHRC
Human Rights Council rapporteurs
26 Nobel Peace Laureates
61% of The Public


U.S. MILITARY

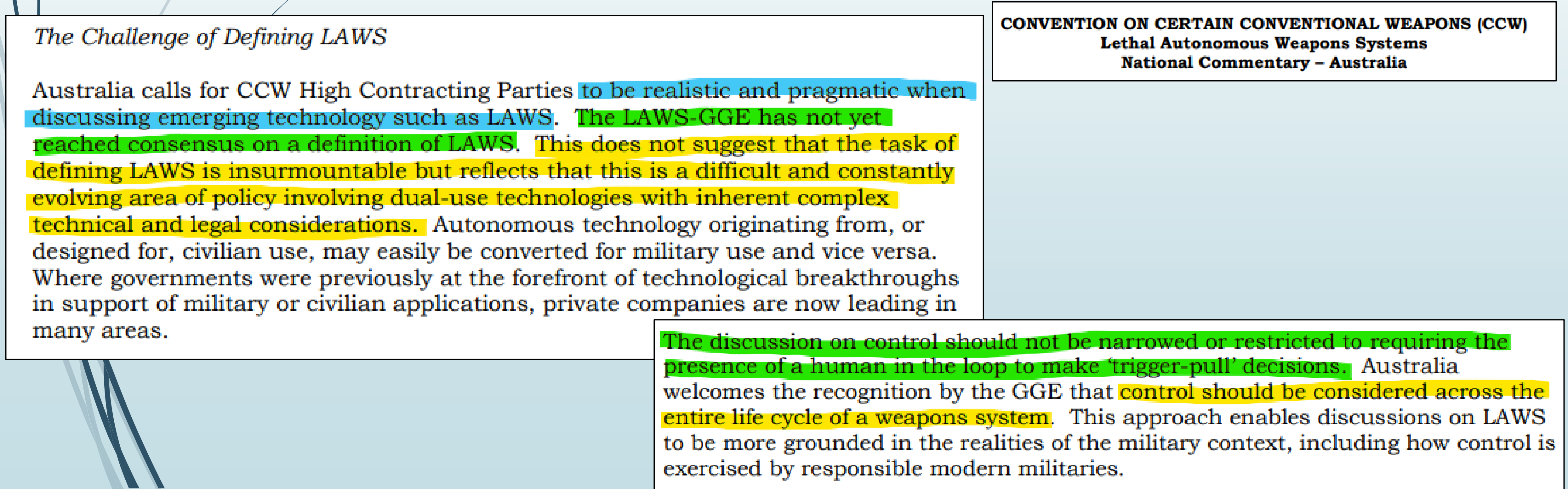
US general warns of out-of-control killer robots

By Ryan Browne, CNN

Updated 0118 GMT (0918 HKT) July 19, 2017

Current state of play as regards regulation?

- Three broad approaches:
  - 1. Existing IHL / LOAC and international law (eg Law of the Sea, Air Law) can manage AWS via application of general principles, interpretation of specific rules, and analogy
    - We will meet a frontier at some point – probably with AI and advanced machine learning – but we are not there yet
    - Australian approach?



CONVENTION ON CERTAIN CONVENTIONAL WEAPONS (CCW)
Lethal Autonomous Weapons Systems
National Commentary – Australia

The Challenge of Defining LAWS

Australia calls for CCW High Contracting Parties to be realistic and pragmatic when discussing emerging technology such as LAWS. The LAWS-GGE has not yet reached consensus on a definition of LAWS. This does not suggest that the task of defining LAWS is insurmountable but reflects that this is a difficult and constantly evolving area of policy involving dual-use technologies with inherent complex technical and legal considerations. Autonomous technology originating from, or designed for, civilian use, may easily be converted for military use and vice versa. Where governments were previously at the forefront of technological breakthroughs in support of military or civilian applications, private companies are now leading in many areas.

The discussion on control should not be narrowed or restricted to requiring the presence of a human in the loop to make 'trigger-pull' decisions. Australia welcomes the recognition by the GGE that control should be considered across the entire life cycle of a weapons system. This approach enables discussions on LAWS to be more grounded in the realities of the military context, including how control is exercised by responsible modern militaries.

Three approaches…

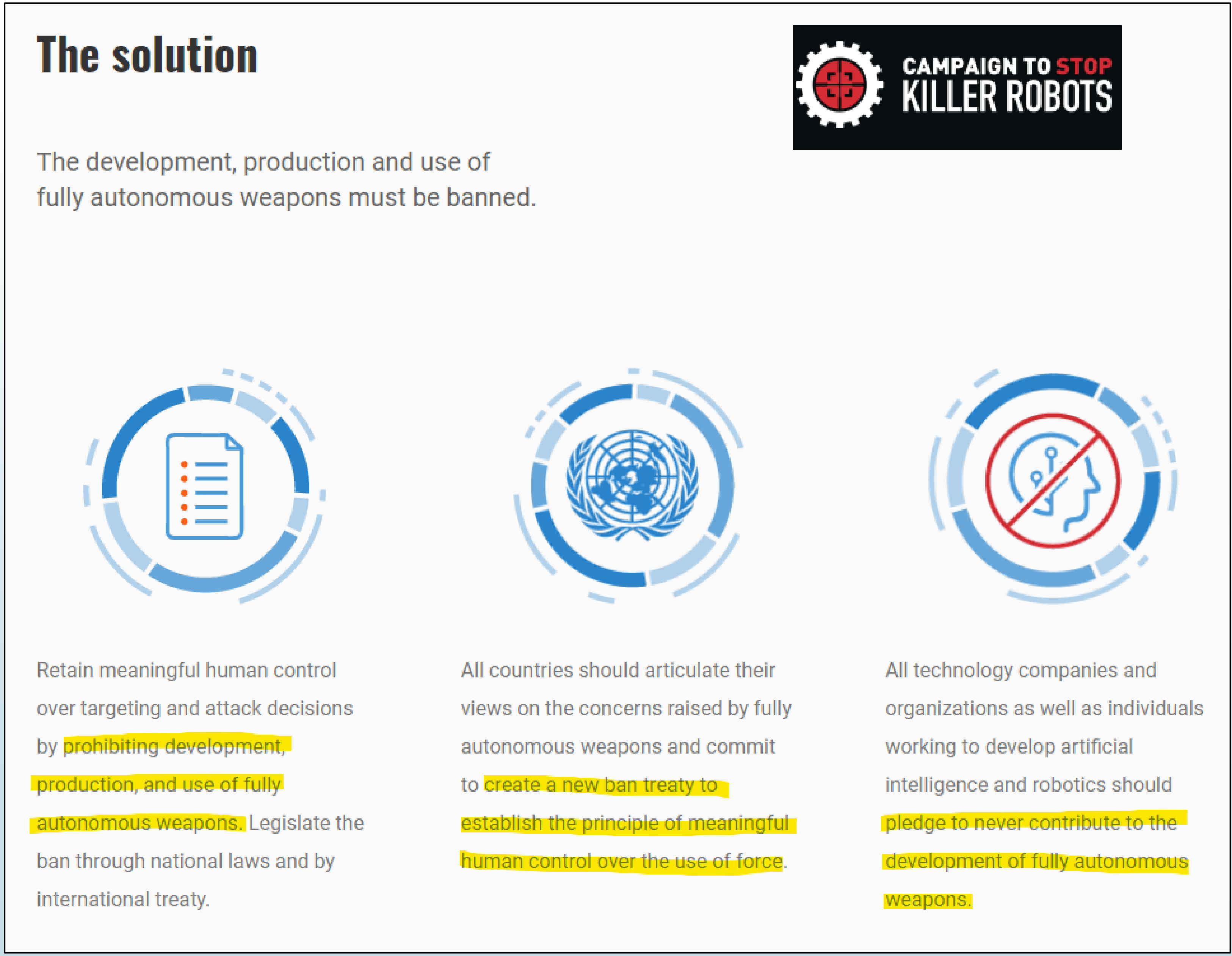
- 2. Existing law is already approaching its technological frontier and we need to start developing sectoral rules now, and then iteratively broaden scope of specific regulation as the technologies develop
  - Start with banning the Terminator, but then wait and see as the technology evolves and we get a sense of what reality might look like
    - Probably means sequencing test rules for **air and maritime**, where the battlespace is less cluttered with civilians and civilian objects and the distinction challenge is less problematic than the 'three block war'?
  - Need to see how the civil legal system grapples with autonomous technologies
    - Driverless cars and trucks, trains, aircraft;
    - Tortious liabilities where decision support systems used, or autonomous decision systems employed – eg in finance, manufacturing etc

What makes the maritime and air-air domains good test beds for establishing regulatory baselines for AWS?

- Less likelihood of civilians and civilian objects in the immediate area of intended effects?
  - Proportionality is less of a concern if you can localize effects in areas where civilians and civilian objects are not present
- Ability to distinguish civilian objects and military objectives is the primary issue, as opposed to distinguishing between civilians and combatants in the urban ‘three block war’
- Less cluttered nature of the battlespace
  - Distinction and discrimination is a more finite task, with bigger ‘things’ and fewer variables
    - A passenger liner is clearly not a warship and sensors + database + system can recognize that
    - But if it has become an enemy auxiliary (eg troop transport)and thus is now targetable, there are a finite number of ships and a data set could accommodate a change in status

Three approaches…

- Complete pre-emptive ban on all fully AWS now, before the technology is developed any further
  - Noting that some examples of simple, but nevertheless ‘human out of the loop’ AWS, already exist
  - State appetite to negotiate a treaty?



The solution

CAMPAIGN TO STOP KILLER ROBOTS

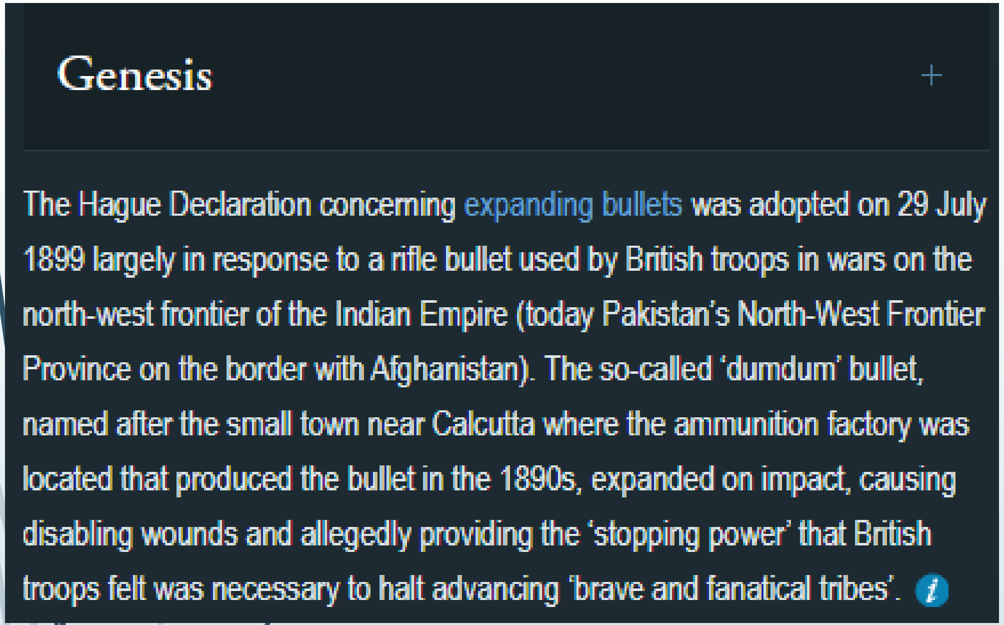
The development, production and use of fully autonomous weapons must be banned.

Retain meaningful human control over targeting and attack decisions by prohibiting development, production, and use of fully autonomous weapons. Legislate the ban through national laws and by international treaty.

All countries should articulate their views on the concerns raised by fully autonomous weapons and commit to create a new ban treaty to establish the principle of meaningful human control over the use of force.

All technology companies and organizations as well as individuals working to develop artificial intelligence and robotics should pledge to never contribute to the development of fully autonomous weapons.

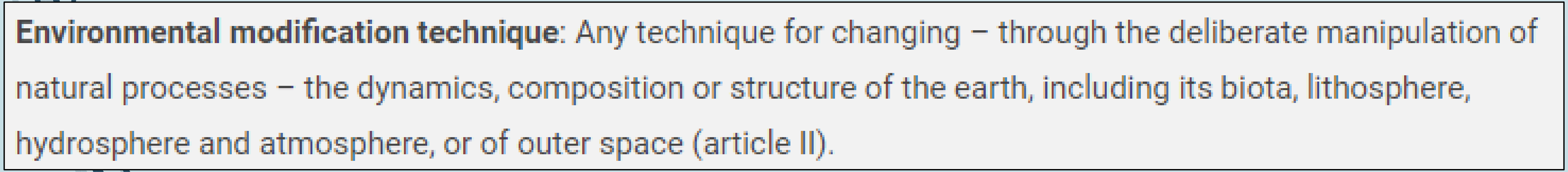
3. What risks attend early comprehensive prohibition?



Genesis

The Hague Declaration concerning expanding bullets was adopted on 29 July 1899 largely in response to a rifle bullet used by British troops in wars on the north-west frontier of the Indian Empire (today Pakistan's North-West Frontier Province on the border with Afghanistan). The so-called 'dumdum' bullet, named after the small town near Calcutta where the ammunition factory was located that produced the bullet in the 1890s, expanded on impact, causing disabling wounds and allegedly providing the 'stopping power' that British troops felt was necessary to halt advancing 'brave and fanatical tribes'.

- 1. Unintended consequences?
  - International community prohibited use of flattening and expanding rounds against enemy forces in 1899
    - But technology has advanced and these types of rounds considered essential in some law enforcement environments to reduce incidental injury
    - What is potential for a complete ban to also remove option of more discriminating systems?
  - ENMOD Treaty 1977 – prohibits use of environmental modification techniques in armed conflict – technology still not there…
    - Now considered to have been a 'look over there and deal with that!' diversion by US and USSR to redirect Non-Nuclear Weapons States away from nuclear-disarmament drive…



Environmental modification technique: Any technique for changing – through the deliberate manipulation of natural processes – the dynamics, composition or structure of the earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space (article II).

Risks of early comprehensive prohibition?

- 2. Degrade perceptions as to the utility of IHL / LOAC more broadly?
  - There is a 'compliance' gap already
  - Does a complete, pre-emptive, prohibition on AWS risk LOAC being seen by operators and governments as 'not fit for purpose' as technology evolves, and thus LOAC becomes discountable?
    - Risk of this perception bleeding across into perceptions about / compliance rates with LOAC more broadly?
    - Risk of mismatch between LOAC prohibition and broader 'social licence' for AI and AWS that reduces own force ('our children') casualty risks?

4. Concluding thoughts?

- At root, is the ‘Terminator’ fear not really about fully AWS, but more as to the **context** in which such AWS might be deployed?
  - If so, consider prohibitions by situation / battlespace context, rather than an early pre-emptive and comprehensive prohibition?
- It is the capacity of an AWS to distinguish between civilian and combatant – rather than presence of ‘meaningful human control’ – that is (I think) the key **legal** (but not necessarily ethical) issue for future regulation
  - If can overcome this challenge – eg a database of all known and accepted vessel targets and a matching enabler sensor suite – is the legal problem of discrimination insurmountable (at least in some domains)?
- Not all of the legal challenges attending AWS are about **future** regulation
  - There are current issues we need to solve – such as whether AWS can be warships
  - But to some extent this is actually an indicator that the existing legal scheme is adequately equipped to deal with AWS for the moment
    - At least until we reach a legal frontier – the point at which the law really does fall silent because it simply can’t comprehend the technology – which might be AI or advanced machine learning