



INTERNATIONAL LAW & CYBER WAR

Prof. Douglas Guilfoyle
UNSW Canberra

OVERVIEW

1. The Australian position
2. Distinctions in international law
3. Deterrence & cyber strategy
4. Why does international law make a difference and how does it work?
5. What is the existing law and can we apply it? Acts short of war, *jus ad bellum*, *jus in bello*.
6. Applying UN Charter law to Stuxnet & Iranian Drones
7. Tallinn Manual on Cyber Warfare & dual use infrastructure
8. Other 'governance' efforts?
9. Does China care?

1. THE AUSTRALIAN POSITION

Prime Minister Turnbull ([22 April 2016](#)):

“An offensive cyber capability housed in the Australian signals directorate provides another option for government to respond. The use of such a capability is subject to stringent legal oversight and is consistent with our support for the international rules based order and our obligations under international law.

Acknowledging this capacity adds a level of deterrence.”



THE AUSTRALIAN POSITION

Prime Minister Turnbull ([22 April 2016](#)):

“An offensive cyber capability housed in the Australian signals directorate provides another option for government to respond. The use of such a capability is subject to **stringent legal oversight** and is consistent with our support for the **international rules based order** and our **obligations under international law**.

Acknowledging this capacity adds a level of deterrence.”



THE AUSTRALIAN POSITION

Australia's Position on the Application of International Law to State Conduct in Cyberspace (2017-2019)

“Existing international law provides the framework for state behaviour in cyberspace. This includes ... the law regarding the use of force, international humanitarian law (IHL), international human rights law, and international law regarding state responsibility.”

“However, Australia recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty, attribution and jurisdiction, given that different actors engage in a range of cyber activities which may cross multiple national borders.”



DISTINCTIONS IN INTERNATIONAL LAW

1. Direct attacks on systems, networks and organisations

If these involve a 'use of force' or an 'armed attack' they are governed by the international law found in the UN Charter **and the law applicable to the use of force in self-defence** ('jus ad bellum').

2. Cyber-support of military operations – disruption and compromise

Governed by the international **law applicable during war**: 'the law of armed conflict' or 'jus in bello'

How can we respond to smaller-scale cyber violations? International law distinguishes: **retorsion, countermeasures and reprisals.**



4. INTERNATIONAL LAW AND CYBER CONFLICT

LAW: WHAT IS IT GOOD FOR?

Does international law determine the conduct of major powers or 'bad actors':

- No.

Whether we think international law works depends on what job we are asking it to do.

Does the world have one morality, culture, language, system of government? No.

- How do we debate or contest the legitimacy of a State's actions without a common morality?
- How do we coordinate State action to solve common problems across diverse governments, cultures, languages?





WHY DOES INTERNATIONAL LAW MAKE A DIFFERENCE?

A global rules-based order addressing security, trade, the environment and human rights:

- reduces friction between States and the likelihood of conflict;
- promotes development and prosperity; and
- provides a framework for cooperation to address complex problems.

A rules-based order favors middle powers like Australia.

Further, we have disproportionate international law expertise for our size.

WHY DOES INTERNATIONAL LAW MAKE A DIFFERENCE?

Even a superpower has an incentive to follow international law (most of the time).

- If it can influence the development of a system of rules that promotes its interest **and** other States' prosperity as well, this is cheaper and more efficient than rule by force (benign hegemon thesis).
- Harder and more costly to impose your rules on others (coercive hegemon thesis).

Whether a hegemon is benign or coercive may depend on your viewpoint.

HOW DOES INTERNATIONAL LAW WORK?

At a minimum international law can be thought of as a **regime** in IR theory:

“Regimes can be defined as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors’ expectations converge in a given area of international relations.”
(S. Krasner, *Power, the State, and Sovereignty*, 1982)

One means for states to **harmonize expectations** about acceptable conduct (setting ‘norms’).

International law provides reasonably certain and stable framework for international relations and gives States a framework **for assessing each other’s actions** and a common language to frame their disputes.

Law has a “legitimacy effect” and a degree of “compliance pull”.

HOW DOES INTERNATIONAL LAW WORK?

Lawyers can be useful in de-escalating tensions. Law can be used to re-frame **political** questions as **technical** ones.

Visions of the law:

- rule book (static)
- **process** of rule-making/development (dynamic)

Model legal manuals: off-the-shelf assessments of what the existing law requires when applied to new developments.

There is strategic advantage in the broad sense to attempting to influence the development of rules: **norm entrepreneurs**.

Hopefully, all players agree to abide by the rules all think are a good idea. If not, some players may be politically de-legitimized (soft power).

HOW DOES INTERNATIONAL LAW WORK?

Even without strong central enforcement international law serves a number of purposes:

- provides an authoritative record of the 'agreed rules of the game' which usually codify past experience;
- tends to 'stack the deck' in favour of major powers, while allowing a process for peaceful change; and
- compliance with international law may not help you win the war as quickly as possible, but it will give you a better chance of winning the peace.



KEY ISSUES:

1. How does international law apply to cyberspace?
2. Should there be a treaty, or treaties, to regulate cyberconflict? What should such a treaty do?
3. What other governance efforts are happening at the international level?
4. Why would a State actor like China care?



THE ROLE OF THE *TALLINN MANUAL*

Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0 (2017)

- work of a (NATO-sponsored) group of independent experts: advisory - a consensus of experts, not the official positions of governments
- examines the international law governing ‘cyber warfare’
- addresses *jus ad bellum* and *jus in bello*, and related issues
- cyber activities below the level of a ‘use of force’ (in UN Charter sense) not addressed
- “Cyber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace pose real and serious threats” – but are not covered
- What is the purpose of such a model manual?

WHAT IS THE EXISTING LAW AND CAN WE APPLY IT?

Tallinn Manual on principles derived from sovereignty:

- A State may exercise control over cyber infrastructure and activities within its territory
- A State **shall not knowingly** allow the cyber infrastructure located in its territory or under its governmental control to be used for acts that unlawfully affect other States
- A State bears international legal **responsibility** for a cyber operation **attributable** to it and which constitutes a breach of an international obligation
- The fact that a cyber operation has been routed via the cyber infrastructure located in a State is **not** sufficient evidence for attributing the operation to that State

1

The rule of “non-intervention” in internal affairs.

“A State may not intervene, including by cyber means, in the internal or external affairs of another State.” (Rule 66, Tallinn Manual)

A foreign cyber-operation against government systems **can** violate the prohibition on intervention in a State's "reserved domain" (domaine réservé).

This is the rule of international law most likely to be broken by cyber means, including in the case of election interference.



ACTS SHORT OF WAR OR ARMED FORCE



What can a government do **short of force** under international law to respond to a foreign cyber-operation that illegally interferes with its internal affairs?

Retorsion – unfriendly, but legal (eg expel diplomats)

Reprisal – a use of force not in self-defence but to punish and deter – this is unlawful

Countermeasures – allows a State to take action that would otherwise be illegal, in response to an earlier wrongful act by another State (eg suspend oil/gas supply).

See the examples given in the Australian “[case studies](#)” paper issued by DFAT.



ACTS SHORT OF WAR: COUNTERMEASURES

A State wronged by an internationally unlawful act may resort to **proportionate countermeasures**, including cyber countermeasures, against the responsible State. Countermeasures **may not use force**.

“In short, they should, to the extent feasible, consist of measures that have temporary or reversible effects. In the realm of cyberspace, this requirement implies that actions involving the permanent disruption of cyber functions should not be undertaken in circumstances where their temporary disruption is technically feasible and would achieve the necessary effect.”

AUSTRALIA'S 'CASE STUDIES' DISCUSSION PAPER

State A proposes a new corporate tax regime. State B objects.

State B's military uses cyber-means to shut down State A's tax office website.

International law tells us:

- a wrongful act has occurred (intervention in A's internal affairs)
- it is attributable to State B (done by its military, an organ of State)
- but it is not an armed attack ...
- therefore non-forceful, proportionate **countermeasures** would be legal
- acts of **retorsion** would also be legal (expel diplomats)
- **reprisals** (bombing the State B's cyber command) would be unlawful

5. CAN CYBER CONSTITUTE A USE OF FORCE OR ARMED ATTACK?

Clausewitz:

“War is an act of force to compel our enemy to do our will”

Consensus

Force includes “kinetic” (violent) means, and threats and coercion

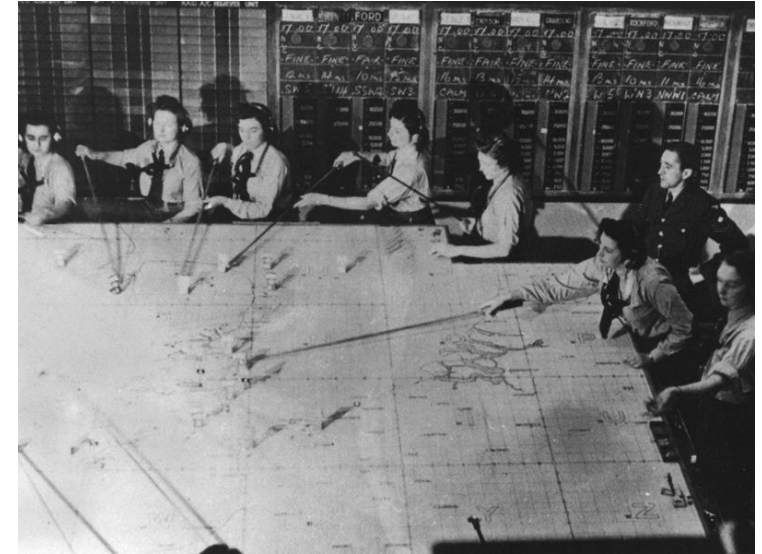
International lawyers generally consider some cyberattacks could be “force” – depending on effects

5. INTERNATIONAL LAW ON THE USE OF FORCE

When is it legal to use military force under the UN Charter system?

2019 “Drone wars” between Iran and the US:

was it legal for the US to conduct a cyber-strike in response to the downing of a US drone?





INTERNATIONAL COURT OF JUSTICE

The law of armed conflict applies to
“any use of force, regardless of the
weapons employed”: *Legality of the
Threat or Use of Nuclear Weapons*
(1996)



UN CHARTER, ARTICLE 2(4)

“All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.

UN CHARTER, ARTICLE 51

“Nothing in the present Charter shall impair the **inherent right of individual or collective self-defence if an armed attack occurs** against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council ...”

Requirements:

- Imminence
- Necessity
- Proportionality

KEY POINTS TO NOTE

Article 2(4) is a very wide ban on the use of force in international relations.

Article 51 sets a high threshold for self-defence (**'armed attack'**).

This obviously leaves a gap where States could be subjected to illegal force and have no 'right of reply'.

Deliberate choice following WWII to prevent escalation. Other options:

- UN Security Council acts (wide Chapter VII powers on peace and security)
- 'self-help': countermeasures and retorsion



INTERNATIONAL COURT OF JUSTICE

What is an **armed attack** giving rise to a right of self-defence? *Nicaragua Case* (1985):

“armed attack must be understood as including not merely action by regular armed forces across an international border, but also ‘the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to’ ... an actual armed attack conducted by regular forces

... The Court sees no reason to deny that ... the prohibition of armed attacks may apply to ... such an operation, [if] because of its *scale and effects*, [it] would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.

But the Court does not believe that ... “armed attack” includes ... assistance to rebels ... [through] the provision of weapons or logistical or other support.”

KEY POINTS FROM THE *NICARAGUA* CASE

An armed attack is the most serious form of the use of force and must be of sufficient **gravity, scale and effects** that it could be considered equivalent to action by regular armed forces and not **a mere frontier incident**.

While every use of force is prohibited, **only the most serious are armed attacks** giving rise to a right of self-defence.

Providing equipment, training or logistical support to rebels is not enough to trigger a right of self-defence but may breach rules on use or threat of force (or violate sovereignty/reserved domain).

JUS AD BELLUM PRINCIPLES

State that is the target of a cyber operation that rises to the level of an **armed attack** may exercise its inherent right of self-defence. Response must be:

- necessary and proportionate
- have imminence and immediacy
- be reported to the UNSC under Article 51 of Charter

But remember an **armed attack** is not just any use of force, but a grave one equivalent to action by conventional forces.

CONTROVERSIAL CASES

Anticipatory self defence: is there “a necessity of self-defence, instant, overwhelming, leaving no choice of means and no moment for deliberation”? (US-UK correspondence over 1837 Caroline incident).

Pre-emptive self-defence: Action to prevent future threats? “If we wait for threats to fully materialize, we will have waited too long” – so called ‘Bush Doctrine’: *National Security Strategy of the United States 2002.*



Retorsion

- legal, but used to express displeasure
- e.g. expel diplomats; prohibit financial services

Countermeasure

- ordinarily illegal, but follows a prior wrong
- Arab States close airspace to Qatar

Sanctions

- collective – authorized by UN Security Council
- unilateral – may be limited by WTO rules

Reprisal

- use of force to deter future conduct
- **always illegal**

Use of force

- necessary and proportionate self-defence
- SC authorization ('breach of the peace')



6. HOW DO WE APPLY INTERNATIONAL LAW REASONING TO STUXNET AND “DRONE WARS”



STUXNET/OLYMPIC GAMES

Geopolitical context

Suspicion Iran seeking to violate NPT obligation not to build nuclear weapons

Iran under IAEA surveillance

UNSC, EU and Congress imposed damaging sanctions

Israel has bombed reactors in Iraq and Syria, and killed Iranian nuclear scientists

2015 – JCPOA agreement freezes enrichment program for 15 yrs.

STUXNET/OLYMPIC GAMES

The virus

Israel & US were responsible, with UK support

Utilized “zero day” exploit that targeted Siemens logic controllers

Varied speed of the centrifuges to cause damage & reduce enrichment levels

Two attacks

June 2009 and March 2010 – Stuxnet 1.0 and 1.001

Dec. 2009 - Iran had 8700 IR-1 centrifuges at Natanz

IAEA notices rapid failure rate – 900-2000 machines in 2 months

Iran retaliates in 2012

Five month attack on US banks

Attack on Saudi ARAMCO destroys 30,000 computer operating systems



ASSESSING STUXNET


Was the Stuxnet attack legal?

Was the Stuxnet attack a prohibited intervention, a use of force, or an armed attack?

If yes, unlawful.

Possibly lawful if Iran had already violated the JCPOA and Stuxnet was done as a **reversible** countermeasure.

Hard to claim it was a countermeasure if done in secret.



ASSESSING STUXNET

Was Iran's response legal?

Iran has a good case it was subject to an illegal cyber operation.

Could it invoke countermeasures? These need to be proportionate and **reversible**.

Hard to claim destructive cyber-attacks intended to be reversible.

Why follow the law?

Contains risk of escalation

Soft power: reputation and legitimacy

2019 DRONE WARS

On 20 June 2019, Iran shot down a United States Global Hawk surveillance drone with a surface-to-air missile over the Strait of Hormuz.

Iran claimed it was in Iranian airspace. The US military said the drone had been over international waters at the time, and condemned what it called an "unprovoked attack".

New York Times: "The Trump administration considered retaliating with military strikes against a handful of Iranian targets, like radar and missile batteries ... But with minutes to spare and planes already headed to their targets, the president abruptly pulled back to prevent what he said would have been the deaths of about 150 Iranians. He also said the number of deaths would not be 'proportionate to shooting down an unmanned drone.'"

Instead (Al Jazeera): "Trump secretly authorised US Cyber Command to carry out a retaliatory cyber attack on Iran ... that disabled Iranian computer systems that controlled its rocket and missile launchers."

2019 DRONE WARS

Was shooting down the drone an “armed attack” or a “mere frontier incident”?

Did the US have a right of self-defence under Article 51 of the UN Charter?

Was the US cyber-attack a “use of force” which could only be legal if it was self-defence?

If we consider the US cyber-attack was a measure short of war – was it a legitimate counter-measure?

Answer depends on:

(1) was Iran shooting down the drone illegal? (Prior wrong)

(2) was the response proportionate? (Proportionality)

(3) was the response non-forceful and reversible? (Prohibition on force, requirement of temporariness)

2019 DRONE WARS

Legal answer depends on the facts:

- If US drone shot down **outside** Iranian airspace – this was an illegal use of force.
- If so, a wrong which might justify proportionate, reversible countermeasures. But did US action measure up?
- If the drone was **inside** Iranian airspace, Iran's action legal – US violated Iranian sovereignty (twice) and is in the wrong.
- On no version of events was this an armed attack/self-defence: Article 51 doesn't apply.



7. INTERNATIONAL HUMANITARIAN LAW (JUS IN BELLO) AND CYBER

How do the traditional rules governing the conduct of hostilities apply to cyber operations?

The dual use infrastructure problem.



JUS IN BELLO: TALLINN MANUAL

International humanitarian law applies to cyberattacks alone, or if the “cyber activity” is part of the armed conflict

Rule 93 – The principle of distinction applies to cyber attacks

International Committee of the Red Cross: “The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians.”

JUS IN BELLO: TALLINN MANUAL PRINCIPLES

The civilian population as such, as well as individual civilians, shall not be the object of cyber attack

Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population, are prohibited

Civilian objects shall not be made the object of cyber attacks

It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature

Starvation of civilians as a method of cyber warfare is prohibited

Cyber attacks that are not directed at a lawful target, and consequently are of a nature to strike unlawful targets and civilians or civilian objects without distinction, are prohibited

DUAL USE INFRASTRUCTURE

Rule 37 – Prohibition on attacking civilian objects

Civilian objects shall not be made the object of cyber attacks. Computers, computer networks, and cyber infrastructure may be made the object of attack if they are military objectives

Rule 39 – Objects used for civilian and military purposes

An object used for both civilian and military purposes – including computers, computer networks, and cyber infrastructure – is a military objective

“Consider a network that is being used for both military and civilian purposes. It may be impossible to know over which part of the network military transmissions, as distinct from civilian ones, will pass. In such cases, the entire network (or at least those aspects in which transmission is reasonably likely) qualifies as a military objective.”



DUAL USE OBJECTS AND PROPORTIONALITY

Rule 113: Proportionality – “A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited.”

“As an example ... consider the case of a cyber attack on the Global Positioning System. The system is dual-use and thus a lawful target. However, depriving the civilian users of key information such as navigational data is likely to cause damage to, for instance, merchant vessels and civil aircraft relying on Global Positioning System guidance.

If this expected harm is excessive in relation to the anticipated military advantage of the operation, the operation would be forbidden ...

An isometric illustration of a city street scene. In the foreground, two people are walking away from the viewer. The person on the left is wearing a grey jacket and a white cap, and the person on the right is wearing a maroon jacket. They are walking on a grey sidewalk. In the background, there are various buildings of different heights and colors (blue, green, brown). There are also some trees and a large blue Wi-Fi symbol in the sky. The overall style is a clean, modern isometric art style.

DUAL USE OBJECTS AND PROPORTIONALITY

Tallinn Manual explains:

“Cyber operations may cause inconvenience, irritation, stress, or fear. These consequences do not qualify as collateral damage because they do not amount to ‘incidental loss of civilian life, injury to civilians, damage to civilian objects’

“Only collateral damage that is excessive to the anticipated concrete and direct military advantage is prohibited. The term ‘excessive’ is not defined in international law. However, ... excessiveness ‘is not a matter of counting civilian casualties and comparing them to the number of enemy combatants that have been put out of action’.”

An isometric illustration of a city with various buildings, trees, and a person in the foreground. The person is wearing a red shirt and blue pants, standing with their back to the viewer, looking towards the city. The city features a mix of modern and classical architecture, with a large blue cloud-like shape in the center. The overall style is clean and modern, with a muted color palette.

DUAL USE OBJECTS AND PROPORTIONALITY

“[The] question is whether the harm that may be expected is excessive relative to the anticipated military advantage given the circumstances prevailing at the time.”

“[Thus] extensive collateral damage may be legal if the anticipated concrete and direct military advantage is sufficiently great. Conversely, even slight damage may be unlawful if the military advantage expected is negligible.”

CONTROVERSY: DOES THE LAW PROTECT CRITICAL CIVILIAN DATA?

Rule 92: ‘A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.’

Requires physical consequences: ‘a majority of [the experts] was of the view that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components.’



CONTROVERSY: DOES THE LAW PROTECT CRITICAL CIVILIAN DATA?

what counts as an **object**? If data is **not** an object, then 'cyber operations targeting data *per se*' don't fall within the definition of 'attack'.

This 'would mean that even the deletion of essential civilian datasets such as social security data, tax records, and bank accounts' would not be prohibited despite the principle 'that the civilian population enjoys general protection from the effects of hostilities.'



CONTROVERSY: DOES THE LAW PROTECT CRITICAL CIVILIAN DATA?

Majority of the Tallinn Manual's international group of experts (IGE) take the view the law has not caught up with this yet: an object is something 'visible and tangible'.

Therefore, attacking vital data in civilian systems would be an act of sabotage not regulated by the laws of armed conflict (*jus in bello*).

Do we need to update the law? New treaty or ... just new interpretation?

Kubo Mačák: a scholar who argues that an 'object' should be interpreted as meaning something the destruction of which is objectively verifiable when attacked.

Michael Schmitt: an IGE author of the Tallinn Manual argues in reply that it is for governments to endorse new interpretations which 'update' the law. The job of the Manual was to reflect the law as it is, not as it should be.

8. OTHER GLOBAL GOVERNANCE EFFORTS



WHAT OTHER GLOBAL GOVERNANCE EFFORTS ARE UNDERWAY?

The Minister for Foreign Affairs, Senator the Hon Marise Payne: Speech at the Lowy Institute 11 March 2019

First, some distinctions:

- Politics is about ‘who gets what’
- Governance is more about the administrative and procedural elements of running a country and implementing policy (‘how do we carry out policy?’)
- Global governance: “the complex of formal and informal institutions, mechanisms, relationships, and processes between and among states, markets, citizens and organizations, both inter- and non-governmental, through which collective interests on the global plane are articulated, right and obligations are established, and differences are mediated” (Thakur & Van Langenhove, 2006)





SENATOR PAYNE: INTERNATIONAL LAW

The most recent attack on our own democratic institutions serves as a reminder that we cannot be complacent about the risks to our sovereignty and the pressing need for **all nations to determine and stand by an agreed set of international rules and norms in cyber space.**

It is now so fundamental to modern life that serious cyber incidents could, if mismanaged, escalate to a form of conflict between states. There is a behavioural **grey-zone in cyber space that unfortunately more actors appear willing to exploit.**

That is why we need greater clarity on the **application of international law in cyber space.**

SENATOR PAYNE: UN EFFORTS

2019 will be a pivotal year ... key UN bodies will meet this year to further strengthen the international framework that governs cyberspace.

The UN Group of Governmental Experts, known as the UNGGE, consists of members chosen by the United Nations to provide broad geographic representation.

The UNGGE ... has made landmark agreements on international security and cyberspace in its five incarnations since being established in 1998. We were very proud to chair the UNGGE in 2013 when it agreed that existing international law applied in cyberspace. Then in 2015 the UNGGE agreed to 11 norms of responsible state behaviour in cyberspace.

We ... are very eager ... to further clarify these rules and norms to reduce this grey zone.



THE 11 UNGGE PRINCIPLES (2015 REPORT)

Non-binding and not especially forceful, include:

- (c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- (d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs ...;
- (f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- (k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State;

...

UN OPEN ENDED WORKING GROUP (2021 REPORT)

34. “States reaffirmed that international law, and in particular the **Charter of the United Nations**, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment”

38. [The OEWG recommends that] “States, on a voluntary basis, continue to inform the Secretary-General of their national views and assessments on how international law applies to their use of ICTs in the context of international security”

Strong focus on confidence building measures and capacity building

UN OPEN ENDED WORKING GROUP (2021 REPORT)

Chair's report noted:

11. Specific principles of international law which were reaffirmed include ... State sovereignty; sovereign equality; the settlement of international disputes by peaceful means ... ; refraining in their international relations from the threat or use of force ... ; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.

12. It was recalled that international law is the foundation for stability and predictability in relations between States. In particular, international humanitarian law reduces risks and potential harm to both civilians and civilian objects as well as combatants in the context of an armed conflict.

10. WHY WOULD A STATE LIKE CHINA CARE ABOUT GLOBAL 'NORMS' OF CYBER 'GOVERNANCE'?

Three warfares:

- public opinion warfare
- psychological warfare, and
- legal warfare.

The three warfares go to questions of legitimacy and soft power.

China is concerned with its external **and** internal legitimacy

Attacking China's external legitimacy is seen as waging information warfare against its internal legitimacy.

China believes arguments over international law count.

THE SHANGHAI COOPERATION ORGANIZATION VIEW

China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan

Concerned with the “three evils”: terrorism, separatism and extremism

Principles proposed to UNGGE (but not adopted) – States should:

cooperate in combating criminal and terrorist activities that use information and communications technologies ... and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment

fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations

promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet

