

ISODARCO

Malicious Cyber Operations: Countermeasures in International Law and their Role in Cyberspace

8 Aug 2025

Danielle Yeow (d.yeow@nus.edu.sg)
Centre for International Law
National University of Singapore



Function of International law



CENTRE FOR INTERNATIONAL LAW
National University of Singapore

“The rules based international order

- recognises sovereign equality of all States ...*
- ..enshrines fundamental principles that promote peace and order eg the territorial integrity of all nations; the peaceful settlement of disputes in accordance with International Law”*
- ...gives all States a stake in the global commons. ... provides a predictable set of rules to advance as well as to defend their interests.*
- ... provide a stable environmental for international trade and investment...”*

Keynote Address by SGP Minister K Shanmugam at the CIL International Law Year in Review 2024 Conference

Is State conduct that relies on cyber means governed by international law?

Applies to States' conduct in cyberspace

- See e.g. 2013, 2015, 2021 GGE reports, 2021 OEWG report, 2021-2025 OEWG Annual Progress Reports and Final Report (July 2025)

What rules and principles of international law applies?

How do they apply?

Art 2(4) UN Charter

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.

When does a cyber operation carried out by a state amount to “threat or use of force” against the territorial integrity or political independence of any State”?

Art 51 UN Charter

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,

When does a hostile cyber operation constitute an “armed attack” that justifies exercise of self-defence? What about a series of cyber incidents that individually fall below the threshold of armed attack?

QUESTIONS



What rules apply or are excluded?



Who is responsible?

evidence, attribution, state
responsibility



Accountability?

How to hold states accountable?
What are the available/permitted
responses?



Third party states?



Non-state parties?

OUTLINE



CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Countermeasures in international law

Substantive conditions

Procedural conditions

Countermeasures in ‘cyberspace’

Collective countermeasures

AI and autonomous cyber operations

- measures taken by a State in response to the internationally wrongful act of another State
- aimed at inducing the latter State to comply with its legal obligations

NOT

- punitive
- reprisals
- retorsion (unfriendly but lawful measures)
- pre-emptive 'anti-AI countermeasures'
- defensive cybersecurity countermeasures

Legal Sources

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore



Customary international law



The International Law Commission (ILC)'s Articles on the Responsibility of States for Internationally Wrongful Conduct (ARSIWA) 2001

Article 22: Countermeasures in respect of an internationally wrongful act

The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of part three.



ICJ jurisprudence (*Gabčíkovo-Nagymaros* case)

“might justify otherwise unlawful conduct “taken in response to a previous international wrongful act of another State and [...] directed against that State.”

Substantive conditions (Art 49-51)

prior
internationally
wrongful act by a
state

Initiated by the
injured state (s)

against the
wrongdoing state

purpose to induce
compliance,
rather than to
punish

non-forcible in
nature, certain
forms prohibited

proportional to
injury suffered,
gravity of act and
the breach

reversible as far
as possible

temporary – until
termination of
wrongful conduct
or reparation

obligations not
affected

Procedural Obligation (Art 52 ARSIWA)

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

before taking countermeasures

- call upon the wrongdoing state to cease the wrongful act or make reparations
- notify the wrongdoing state and offer to negotiate.



exception - when urgent countermeasures necessary to preserve its rights



to cease or suspend countermeasure if internationally wrongful act has ceased or dispute is before tribunal or court.

Countermeasures in Cyberspace



CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- Features of ICTs present challenges in interpretation and implementation of international law
 - dual use nature of certain ICTs eg communication infrastructure and encryption algorithm;
 - anonymity of the threat actor;
 - speed, immediacy and instantaneous effects over long distances across territorial and geographical boundaries;
 - interconnectivity between different technologies and devices;
 - non-physical nature of many online goods and services that are facilitated or provided by ICTs eg hospital databases and social media; and
 - the quality and apparent authenticity of “fake and manipulated content”.

Question

Are current substantive and procedural requirements compatible with or too restrictive for countermeasures to be satisfactorily or effectively applied in the cyber context?

Challenges

- Does the cyber operation amounts to internationally wrongful act by a State that gives rise to state responsibility? (cyber espionage, cyber crime, misinformation/disinformation operations, cyber attack, “defend forward” preemptive measures)
- Attribution (technical, political, legal)
- Measures taken in response
 - Ensure effectiveness of injured State’s response (proportionality assessment, notification and prior demand v urgency)
 - Avoid spillover side effects on third States, private entities and individuals

See States' public articulations
on issue of countermeasures
eg notification, reversibility,
attribution and evidence



Cyber Law Toolkit

- List of articles - International cyber law: interactive tool

Official Compendium of Voluntary National Contributions on how International law Applies to the use of ICTs – Annex to UNGGE Report 2021

Submissions of national views to OEWG (2019-2021) and OEWG (2021-2015)

Other References

Statements delivered at the OEWG (agenda item: International Law)

Cyber Law Toolkit

List of articles - International cyber law: interactive tool

UNIDIR Cyber Policy Portal
<https://cyberpolicyportal.org/>

CASE STUDIES

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

2007 Estonia
cyber attacks

NotPetya and
Collective
Attribution

Collective Countermeasures

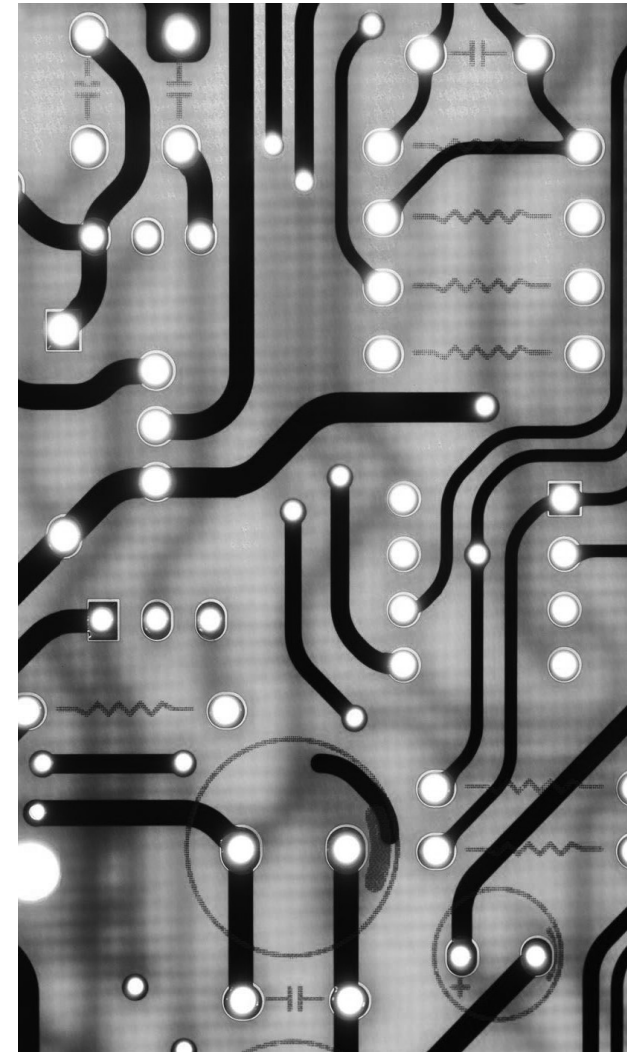
CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- Countermeasures by states **other than the injured state at the request** of the injured state for assistance.
- Is this permitted under international law?
- Rationale for supporting collective counter-measures and vice-versa?

To be distinguished from:-

- Situation involving prior violation of an *erga omnes* obligation by the wrongdoing state (Denmark, Costa Rica, Colombia, Austria) Art 54
- Measures taken in collective self defense including measures taken in cyberspace (Canada),



See States' public articulations on issue of collective countermeasures



Cyber Law Toolkit

- List of articles - International cyber law: interactive tool

AI and autonomous cyber operations



CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- complexities in legal analysis and application compounded by the risks associated with integration of AI into cyber operations and responses
 - Attribution assessment
 - Proportionality assessment
 - Imminence assessment
- Implications wrt objective of countermeasures
 - Inducing compliance vs. escalation

Way forward?

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore



Countermeasures is part of the wider debate on how international law applies to states' activities in cyberspace



OEWG Final Report Recommendations

States to continue discussions at the future permanent mechanism on how international law applies in the use of ICTs. ("New UN Global Mechanism")

States are encouraged to continue to voluntarily share their national views and positions, which may include national statements and State practice, on how international law applies to the use of ICTs.



Proposal for dedicated thematic group on international law dropped from Final Report

Way forward?

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore



“recoding international law” via national statements and regional statements on the application of international law in cyber

<https://www.ejiltalk.org/the-application-of-international-law-in-cyberspace-a-debate-that-is-recoding-international-law/>



building convergence through multistakeholder dialogue, track 1.5 dialogue, regional, plurilateral initiatives



**Academia eg
Tallinn Manual 3.0
Oxford Process**

CONSIDERATIONS?

Q & A