POWERS

Peace, War and the World in European Security Challenges

Cyberspace, International Law and Self-Defense

Paolo Bargiacchi

Professor of Public International Law at Kore University of Enna, Italy

Co-funded by the Erasmus+ Programme of the European Union

The Fifth Operational Domain

Land, sea, air, space and cyberspace

Similarities and differences (Welch, 2011)

Embedded in all the other domains

Constructed by man and changing from moment to moment

Co-funded by the Erasmus+ Programme of the European Union

New Phenomena

Cyberspace and information society are (relatively) new for international relations and international law

Principles and rules were created for geophysical domains

International law is not still developed to fully address States and non-State actors' conducts and operations in cyberspace

Co-funded by the Erasmus+ Programme of the European Union

Information and Communications Technology

Widespread agreement in applying existing international law in cyberspace whenever possible

2013 UN-mandated GGE: “international law and the UN Charter are applicable and essential to maintaining peace and promoting an open, secure, peaceful and accessible ICT environment”

Co-funded by the Erasmus+ Programme of the European Union

2018 UNGA Resolution 73/27

Rules and principles aimed at defining scope and content of responsible behaviours of States in the use of ICTs

Use of ICTs may threaten or breach international peace and security and trigger UN Security Council Chapter VII powers and self-defence under Article 51

Co-funded by the Erasmus+ Programme of the European Union

UNGAR 73/27 and State responsibility

Not knowingly allow their territory to be used by other States and non-State actors for internationally wrongful acts

Not using proxies to commit internationally wrongful acts using ICTs

Duty to ensure their territory is not used by non-State actors

Co-funded by the Erasmus+ Programme of the European Union

UNGAR 73/27 and critical infrastructure

Take appropriate measures to protect C.I. (medical facilities, financial services, energy, water, etc.) from ICTs threats

Respond to appropriate requests for assistance

Take reasonable steps to ensure the integrity of the supply chain

Not to allow malicious ICTs activity against other States C.I. emanating from their territory

Co-funded by the Erasmus+ Programme of the European Union

Role of the United Nations

Open-Ended Working Group established by UNGAR 73/27

- Involving all interested UN Member States (2019/2021 mandate)
- further develop rules, norms and principle of responsible behaviour of States
- study existing and potential ICT threats and possible cooperative measures
- Final Substantive Report adopted on 12 March 2021 available at https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Co-funded by the Erasmus+ Programme of the European Union

OEWG Final Substantive Report

Main conclusions

- States are increasingly concerned about malicious use of ICTs
- Harmful ICT incidents are more and more frequent and sophisticated and are constantly evolving and diversifying
- Use of ICTs in future inter-state conflicts is becoming more likely
- Non-State actors (including terrorists and criminal groups) have ICT capabilities previously only available to States

Co-funded by the Erasmus+ Programme of the European Union

OEWG Final Substantive Report

Main conclusions

- ICT activities may have devastating security, economic, social and humanitarian consequences on critical infrastructure
- Urgency of implementing and further developing cooperative measures
- Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability
- Norms do not replace binding international law but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs

Co-funded by the Erasmus+ Programme of the European Union

Role of the United Nations

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of International Security

- Working in parallel with the OEWG (2019/2021 mandate)
- Chaired by Brazil and composed by 25 Members States (P5, Australia, Germany, India, Japan, Jordan, Kenya, Morocco, Norway, South Africa, etc.)
- Essentially addresses same issues dealt with by the OEWG

Co-funded by the Erasmus+ Programme of the European Union

Principles of International Law

International law, including the principles of sovereignty and non-intervention, does apply to States' activities in cyberspace

How these principles actually apply is unclear and States are also often ambiguous in invoking the law (Moynihan, 2019)

Policy of silence and ambiguity with a view to preserving operational flexibility (Efrony & Shany, 2018)

Co-funded by the Erasmus+ Programme of the European Union

State Sovereignty

Legal rights to territorial integrity and political independence flow from State sovereignty

Does any unauthorized cyber operation or activity against or Within a State amount to a violation of its sovereignty?

State practice is not still clearly oriented and uniform

Co-funded by the Erasmus+ Programme of the European Union

State Sovereignty

UNGAR 73/27 (Preamble): “State sovereignty and international norms and principles that flow from sovereignty apply to State Conduct of ICT-related activities”

Tallinn Manual 2.0: any unauthorized cyber conducts should be unlawful because in breach of State sovereignty (expansive approach)

Co-funded by the Erasmus+ Programme of the European Union

State Sovereignty

Many States took a ‘wait and see’ restrictive approach

Some unauthorized cyber conducts may be unfriendly but not also unlawful because they do not violate the principle of sovereignty

UK Attorney General, 2018: “not all exercises of authority Carried out without consent” of the target-State amount to a violation of its sovereignty

Co-funded by the Erasmus+ Programme of the European Union

State Sovereignty

Why a restrictive approach to sovereignty in cyberspace?

Many cyber intrusions are not harmful for the target-State

Lack of binding clear rules = more legal freedom of action in collecting data and information from foreign States' systems and databases

Co-funded by the Erasmus+ Programme of the European Union

Non-intervention

Article 2(7) of the UN Charter

Widespread consensus among States on its applicability in cyberspace

Intervention is “any type of [armed, economic, political or any other type of] measures to **coerce** another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind”

1970 UNGAR 2625 (XXV)

Co-funded by the Erasmus+ Programme of the European Union

Non-intervention

Coercion is the hallmark of prohibited intervention

Coercion must bear on inherently sovereign "matters in which each State is permitted to decide freely"*:* formulation of foreign policy, stability of its own financial system, operation of Parliament, etc. (ICJ, *Nicaragua*, § 205)

Netherlands, 2019: "coercion means compelling a State to take a course of action that it would not otherwise voluntarily pursue"

Co-funded by the Erasmus+ Programme of the European Union

Intervention and Interference

Western States: interference (i.e., non-armed and non-coercive influence) may be unfriendly but it is not unlawful intervention: e.g., traditional messaging setting forth a State's position on a foreign elections is not coercion

Non-western States: armed or otherwise coercive intervention as well as **any kind of interference** in domestic affairs are always prohibited by international law

Co-funded by the Erasmus+ Programme of the European Union

Foreign Cyber Interference in Elections

"Cyber operations intended to affect the State's ability to conduct an election by targeting either state-end electoral administration and infrastructures or the voters' ability to properly cast a ballot are coercive in nature" (Schmitt, 2020)

Australia, 2019: "cyber operations to manipulate the electoral system to alter the results of an election" violates art. 2(7) of the UN Charter

Claiming legal attribution of cyber conducts is complex and troublesome
Inter-States political naming and blaming

Co-funded by the Erasmus+ Programme of the European Union

Self-defence in Cyberspace

Major problems in interpreting and applying self-defence

What is a cyber “armed attack” under Article 51?

When a cyber threat is “imminent”?

Anticipatory **vs** pre-emptive self-defence

Co-funded by the
Erasmus+ Programme
of the European Union

Self-defence in Cyberspace

Cyber operations should be assessed by standards applied to physical/kinetic armed attacks in the real world

BUT

“the rapidity of cyberattacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles on self-defence” (Australia, 2019)

Co-funded by the Erasmus+ Programme of the European Union

Imminence in Cyberspace

Imminent = armed attack that is about to be launched

Imminent attacks engage the right of self-defence because “a State need not wait to suffer the actual blow before defending itself, so long as it is certain the blow is coming” (O’Connell, 2002)

Is the “imminent” standard applied in real-world also appropriate in cyberspace?

Co-funded by the Erasmus+ Programme of the European Union

Imminence in Cyberspace

Cyber armed attacks “might be launched in a split-second” leaving no opportunity for the target State to effectively defend

Australia, 2019: is it serious to suggest “that a State has no right to take action before that split-second”?

Australia, 2019: States have the right to “act in **anticipatory** self-defence when the attacker is clearly committed to launching an armed attack and the victim will lose its last opportunity to effectively defend itself unless it acts”

Co-funded by the Erasmus+ Programme of the European Union

Pros and Cons

Hostile cyber conducts are
instantaneous, non-physical and invisible

Cyber-imminence would upset the use of force
in self-defence from **defensive** to **offensive**

Self-defence **before** any attack effectively occur and **even if**
uncertainty remains as to the time and place of the cyber armed attack

Co-funded by the
Erasmus+ Programme
of the European Union

Expansive Theories on Self-defence

Expansive theories on self-defence in the aftermath of 9/11

Most States support **anticipatory** (from imminent attacks),
If not **pre-emptive** (from remote attacks), self-defence
from NSA's threats and attacks (e.g., terrorist groups)

Co-funded by the
Erasmus+ Programme
of the European Union

Expansive Theories on Self-defence

Expansive theories: self-defence is lawful even if there is “no specific evidence of where an attack will take place or of the precise nature of an attack [but there is however] a reasonable and objective basis for concluding that an armed attack is imminent”

Brian Egan, former Legal Adviser, US Department of State
Daniel Bethlehem, former Legal Adviser, UK Foreign Office

Co-funded by the Erasmus+ Programme of the European Union

Temporal or Necessary Imminence?

Traditional concept: the armed attack must really be about to occur in **temporal terms**

Expansive concept: “armed attack will be regarded as imminent if responding to the attack is **necessary now** regardless of when and how exactly the attack will take place” (Milanovic, 2020)

Co-funded by the Erasmus+ Programme of the European Union

A Modern Law of Self-defence

Many States (Australia, UK, US, etc.) support a “modern law of [anticipatory or pre-emptive] self-defence” founded on revised and (greatly) expanded notion of (necessary) imminence

Modern law = offensive actions for preventing and deterring future threats rather than defending from imminent attacks?

Co-funded by the Erasmus+ Programme of the European Union

Modern Self-defence in Cyberspace

Unconventional security threats brought by NSA justify the need for a modern law of self-defence in the real world

Cyberspace is a fertile ground for applying and further expanding scope and content of the modern law of self-defence

Self-defence in cyberspace might be decoupled from any kind of temporal standard/limit (on-going, imminent, remote, etc.)

Co-funded by the Erasmus+ Programme of the European Union

A New Legal Landscape?

Would expansive theories on self-defence in real world and cyberspace change the legal landscape of the UN Charter on the use of force in international relations?

UN Charter: lawful use of force is an exception

Tomorrow: will the lawful use of force be the new general rule?

Co-funded by the Erasmus+ Programme of the European Union

Conclusions

States are searching for more legal leeway to better Struggle against unconventional security threats (non-State actors, cyber operations, etc.)

States need a new and more flexible legal framework on the use of force for the future

Co-funded by the Erasmus+ Programme of the European Union

Conclusions

Cyberspace might be the best new ground for struggling against each other in a more silent way and at lower costs

Less legal certainty and more legal flexibility in future international law?

More freedom of action = more hostile or armed cyber conflicts and incidents in international relations?

Co-funded by the Erasmus+ Programme of the European Union

Thank You!

bargiacchi71@yahoo.com /// paolo.bargiacchi@unikore.it

https://unikore.academia.edu/PaoloBargiacchi

https://papers.ssrn.com/sol3/results.cfm

http://powers-network.vsu.ru/en/publications

Co-funded by the Erasmus+ Programme of the European Union

References

BARGIACCHI, *Sovereignty, Non-intervention and Self-defence in Cyberspace*, in *Rivista della Cooperazione Giuridica Internationale* (forthcoming) and http://powers-network.vsu.ru/en/publications

WELCH, *Cyberspace - The Fifth Operational Domain*, Institute for Defense Analyses, 2011, https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf

MOYNIHAN, *The Application of International Law to State Cyberattacks*, Chatham House, 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Co-funded by the Erasmus+ Programme of the European Union

References

EFRONY-SHANY, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, *The American Journal of International Law*, vol. 112, 2018, p. 583 ss.

UK Attorney General's Speech, *Cyber and International Law in the 21st Century* (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, at https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Co-funded by the Erasmus+ Programme of the European Union

References

The Netherlands, *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*, at https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

SCHMITT, *Foreign Cyber Interference in Elections: An International Law Primer, Part I-III* (Oct. 16-19, 2020), at https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-i/

O'CONNELL, *The Myth of Pre-emptive Self-Defence*, ASIL Task Force Papers, August 2002, at http://www.asil.org/taskforce/oconnell.pdf

Co-funded by the Erasmus+ Programme of the European Union

References

Australia, *2019 International Law Supplement*, *Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace*, at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html

EGAN, *International Law, Legal Diplomacy, and the Counter-ISIL Campaign: Some Observations*, in *International Legal Studies. U.S. Naval War College*, vol. 92, 2016, p. 235 ss.

MILANOVIC, *The Soleimani Strike and Self-Defence Against an Imminent Armed Attack* (Jan. 7, 2020), at https://www.ejiltalk.org/the-soleimani-strike-and-self-defence-against-an-imminent-armed-attack/

Co-funded by the Erasmus+ Programme of the European Union

References

UK Attorney General's Speech, *The Modern Law of Self-Defence* (Jan. 11, 2017), at https://www.ejiltalk.org/the-modern-law-of-self-defence/

Australia Attorney-General's Speech, *The Right of Self-Defence Against Imminent Armed Attack in International Law* (May 25, 2017), at https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/

MILANOVIC, *The Soleimani Strike and Self-Defence Against an Imminent Armed Attack* (Jan. 7, 2020), at https://www.ejiltalk.org/the-soleimani-strike-and-self-defence-against-an-imminent-armed-attack/

UNGA Resolution 73/27, 5 December 2018, at https://undocs.org/en/A/RES/73/27

Co-funded by the Erasmus+ Programme of the European Union

References

UK Attorney General's Speech, *The Modern Law of Self-Defence* (Jan. 11, 2017), at https://www.ejiltalk.org/the-modern-law-of-self-defence/

Australia Attorney-General's Speech, *The Right of Self-Defence Against Imminent Armed Attack in International Law* (May 25, 2017), at https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/

AKANDE-ANTONIO-DE SOUZA DIAS, *Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond* (Jan. 5, 2021), at https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/

Co-funded by the Erasmus+ Programme of the European Union