22 AUGUST
2019

LEGAL AND REGULATORY LIMITATIONS AND CHALLENGES IN CYBER SPACE

FUTURE OF CYBER SECURITY

CYBERSPACE : AN INTEGRAL PART OF HUMAN LIFE

- Global economic, societal, and geopolitical systems
- It is used in all aspects of government and individuals daily life activities
  - (policymaking, operations, personnel affairs, public relations, research, development, commerce, economy, entertainment,…)
- It is an **essential infrastructure** that supports various operations across other domains: land, sea, air, and space.
- Security of cyberspace: critically important element to achieve any mission
- Effective operations in this domain are as important as those in others

CYBER THREATS

- Misuse and abuse of this complex borderless space affect vital state interests in the physical world, including national security, public safety, and economic development.
- International law didn't deliver the convenient answer yet
- More than 20 years after the creation of the internet, state agreed on the basic hypothesis **that international law applies to cyberspace (2013)**
- Nevertheless this agreement was expressed in the form of a non-binding report of a group of government experts (GGE) established by the united nations (UNGA)

INEFFICIENT RECOGNITION

- The group was composed of representatives of 15 UN member states, including the three ‘cyber superpowers’ china, Russia, and the united states.
- Still, the report poses more questions than it answers.
- International law is supposed to apply, but which international law?
- Although the group recommended the importance of the UN charter, several of its members have questioned the applicability of a prominent subdomain of international law
  - (the law of armed conflict to cyber operations)

STATES' AWARENESS

- Calls for cooperation regulation and legal frameworks
- WISIS – Tunis
- **Commonwealth cyber declaration**
- ***London, UK, 2018.*** Http://thecommonwealth.Org/commonwealth-cyber-declaration
- **Cyber security: Paris call of 12 November 2018 for trust and security in cyberspace**
- **Declaration by the high representative on behalf of the EU on respect for the rules-based order in cyberspace**
- **New EU sanctions to target malicious external cyber-attacks may 2019**

CYBER THREATS: ANOTHER GLOBAL CHALLENGES

- **Global Challenge: Cannot be adequately addressed by any single actor, alone.**
  - **Climate change, international terrorism**
- **It necessitate a framework for international co-operation.**
- **International law affords a framework, in order to protect international society**
  - **- Establishes constraints**
  - **- guarantees a sphere of autonomy for each actor (state or international bodies)**
  - **- lay down shared boundaries of acceptable conduct in international relations**
  - **- preserve important space for diplomacy and negotiation**
- **States may generally act freely but in case of a opposing rule of law**

SOURCE OF THREATS

- Technical
- Legal
- Intrinsic to the environment
- Human
- States' conduct

CHALLENGES

- Continuous follow up: imposed by the rapid and ever evolving nature of the ICT's
- Managing issues related to the open, complicated and trans border nature of the internet
- Deal with the attribution problem (for proof and liability)
- Protecting human rights endangered by new techniques of personal data processing
- Cope with the evolving power of the private sector defying the states' one
- Blurring distinction lines : endangering peace and impeding elaboration of law

CHALLENGES

- Resistance of Cyber security to codification in a comprehensive multilateral binding convention
- In 1996, France proposed the : “ charter for international cooperation on the internet”
- In 2011 and 2015, two proposals by Russian Chinese initiative for a “code of conduct for information security”
- None of these proposals was met with much enthusiasm

LEGAL CHALLENGES : BALANCING, REDEFINING AND RESHAPING THE FEATURES OF SOME CONCEPTS

- Establish a balance between rights and obligations
- Regulate boundaries between private and public sectors
- Regulate content becoming global threat (Children pornography, fake news)
- Review some basic legal concepts, and principles such as:
  - Right of privacy
  - Intellectual property
  - Sovereignty
  - State responsibility: national & international
- Now: trend of Legislations to take on the topic of cyber security as a whole, that may help in giving a legal definition to cyber security best practices

CHALLENGES

- Reluctance of states to act to generate new rules:
- Visible Reluctance of states:
- - to contribute towards the development of cyber customary international rules.
- - to offer clear expressions of “opinio Juris” on matters related to cyber security.
- Complexity of space and relationships (states, sectors, technologies)

Indicators of states reluctance

- Moving away from the creation of binding treaty or customary rules
- Adoption of normative activity outside the scope of traditional international law.
- Tendency of States' representatives in GGE to use the term 'norms'.
- (In the un GGE report, the group touted the advantages of voluntary, nonbinding norms of responsible state behavior' claiming they:
  - Prevent conflict in cyberspace
  - Foster international development
  - Reduce risks to international peace and security
- The report recommended clearly non-legal binding norms
- Nevertheless, these norms have received very limited agreement

ACTUAL LEGAL LANDSCAPE

- International law apply to states' conduct in cyberspace
  - Efficient application allows for adaptation to new situations and occasions
  - International court of justice (ICJ) states that existing provisions of the international law of the use of force:
    - "Apply to any use of force, regardless of the weapons employed"
- The 1992 constitution of the international telecommunication union
- The 2001 Budapest convention on cybercrime and its 2006 protocol on xenophobia and racism
- The 2009 shanghai cooperation organization's information security agreement;
- The 2014 African union's cyber security convention
- The GDPR of the EU

NON STATES INITIATIVES

- **Microsoft's cyber norms comprehensive proposal:** international cybersecurity norms: reducing conflict in an internet-dependent world was published in December 2014.
- The aim of this white paper was to reduce the possibility of nation states use of ICTs' products and services as part of military operations'
- **The Tallinn manual project :** A non-binding document'.
- on the international law applicable to cyber warfare.
- auspices of the nato cooperative cyber defense centre of excellence (ccd coe), but it reflects the views of the experts not the states or institutions
- It focused on the law on the use of force (jus ad bellum) and the law of armed conflict (jus in bello)
- The two initiatives have state-centric approach and put forward standards of state behavior
- **Non-state origin and expressly non-binding nature.**
- WORLD FEDERATION OF SCIENTISTS PERMANENT MONITORING PANEL ON INFORMATION SECURITY – Erice- declaration on principles for cyber stability and cyber peace

INTERNATIONAL LANDSCAPE

- A clear emphasis on:
- Importance of critical infrastructure
- Application of norms developed within the UN as foundation for international peace and security
- Promoting the widespread acceptance and implementation of:
- - international norms of responsible behavior
- - confidence-building measures in cyberspace
- Application of international law to:
  - the use of ICTs by states
  - human rights
- Need to involve Private sector (Liability of manufacturers)

AN EXAMPLE OF LEGAL HARD MISSION: GDPR'S FACTS

- More than four years of negotiations
- Over 4,000 amendments
- Adopted in may 2016 came into force in may 2018
- Massively impact the financial services sector
- The legal framework to govern the way companies handle data generated by EU citizens
- The regulation is not restricted to countries within the EU
- It applies to the EU citizens' data regardless of where the person or data is located
- Its implications stretch right of EU citizens across the globe
- May be the law responses to large scale data breaches

CYBER NATIONAL LEGISLATIONS

Actual landscape

- Protection of personal data
- Protection of vulnerable social groups (children)
- Data processing and security
- Authentication of electronic records
- E- commerce
- Consumer protection online
- Legal recognition of electronic records
- Legal recognition of digital signatures
- Retention of electronic record
- Security procedure for electronic records and digital signature
- Licensing and regulation of certifying authorities for issuing digital signature certificates
- Liabilities (public & private)

- National strategies and policies build on existing efforts

THE FUTURE: REGULATION ON THE WAY

- **Cyberspace is not the first new phenomenon to have resisted the development of global regulation**
- **Despite the strong initial reluctance of the dominant spacefaring states the domain of outer space is subjected to a binding legal regime**
- **The norms put for the Antarctica in the 1960s and 1970s to conserve living and non-living resources of environment evolved to a binding protocol ratified by all key stakeholders.**
- **The first international conventions on nuclear safety were adopted three decades after the launch of the first nuclear power plant**
- **With states' improved comprehension of the new situation, their willingness to subject themselves to binding rules usually increases.**

- **INDICATOR: 2015 - THE US AND CHINA NEGOTIATIONS OF A BINDING ARMS CONTROL TREATY FOR CYBERSPACE**


THANK YOU