

Content

Sovereignty	7
1. Introduction	7
2. Principle or a standalone rule?	7
3. Threshold of breaching sovereignty	8
4. Cases	9
Jurisdiction	10
1. General	10
2. Types of jurisdiction in public international law	10
3. When states may or must claim jurisdiction	11
4. Territorial, and extraterritorial, jurisdictional claims	12
5. Briefly about the relationship between sovereignty and jurisdiction	12
6. A look towards the future	13
7. Cases	13
State Responsibility	15
1. Introduction	15
2. The Scope of State Responsibility	15
3. The Elements of State Responsibility	16
3.1. Attribution	16
3.2. Ultra vires acts	17
3.3. Attribution of private acts to the state	18
3.4. Breach of an International Obligation of the State	19
3.5. Circumstances Precluding Wrongfulness	21
3.5.1. Consent	21
3.5.2. Self-defence	21
3.5.3. Countermeasures	22
3.5.4. Force majeure	22
3.5.5. Distress	23
3.5.6. Necessity	24
4. Invocation of Responsibility	24
5. The Consequences of International Responsibility	25
6. State Responsibility and Cybersecurity	26
7. Conclusion	28

Use of Force	29
The use of force in international law and the use of international law in cyberspace	29
1. The use of force in international law	29
2. The use of international law in cyberspace	29
3. Charter of the United Nations, 26 June 1945	31
4. The North Atlantic Treaty, Washington D.C., 4 April 1949	32
5. The Draft Articles on Responsibility of States for Internationally Wrongful Acts, The International Law Commission, UN Doc A/56/10	32
6. Tallinn Manual on The International Law Applicable to Cyber Warfare	34
7. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations	39
8. The Cyber Law Toolkit	40
9. The Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States	41
10. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	41
11. International Court of Justice	41
12. International Criminal Tribunal for the former Yugoslavia	50
13. United Nations	50
14. NATO	54
15. European Union	55
16. Literature	56
Critical Infrastructures	59
1. Introduction	59
2. Enforcement	59
3. General requirements	69
4. Sector-specific requirements: the electricity sector	182
Artificial Intelligence: Liability, Digital Content and Autonomous Systems	216
Communication Artificial Intelligence for Europe	216
1. Introduction – embracing change	216
2. The EU's position in a competitive international landscape	219
3. The way forward: an EU initiative on AI	220
4. Conclusion	232
Commission Staff Working Document on the liability for emerging digital technologies	233
1. Introduction	233

2. Landscape of Existing applicable rules and underlying principles from existing legislation or jurisprudence	235
3. The specific characteristics of emerging digital technologies	240
4. Case studies analysis	241
5. Questions for further analysis	247
6. Next steps	250
ANNEX I – Specific Characteristics of Emerging Digital Technologies	251
ANNEX II – List of EU Legislation	252
List of other relevant non-legislative texts concerning artificial intelligence in the European Union	259
Working document on the free flow of data and emerging issues of the European data economy	260
Part 1: Context and purpose of this document	260
Part 3: Data Access and Transfer	261
Part 4: Liability	261
Recommendation for Civil Law Rules on Robotics	267
Directive on digital content and digital services	288
Commission delegated regulation on unmanned aircrafts	367
Resolution on Autonomous weapon systems	392
Standardisation, Certification	395
Introduction	395
The Relevant Legislation	396
See also	435
Digital Discovery	436
Data retention	436
1. Introduction	436
2. Judgments of courts on data retention	442
3. State of play in the member states - data retention	469
4. New proposals on data retention	473
Electronic evidence	476