MASTERCLASS 'Dialogue of disciplines' – 27/29 January 2021
Information about the contribution from the participating Masters (*)

1.GENERAL INFORMATION	
-Denomination of the Master	Master 2 International Relations: Borders- Cooperation and Conflicts
-University	Science Po Strasbourg
-N.of participants	Total in master FRONT: 35 Group 1: 14
-Name and e-mail address of the director of the master	birte.wassenberg@unistra.fr
-Name and e-mail address of the students' contact person	Johanfredsted(at)ymail.com rdichuta@gmail.com

2. CONTRIBUTION TO THE MASTERCLASS	
-Title	Cooperation against cybercrime in Europe
-Summary of the main contents	Cybercrime is a new national security threat that needs to be taken into account. It is within this dynamic that the Council of Europe drafted in 2001 the Budapest Convention on cybersecurity. This international treaty aims to harmonize national laws at the same time as it seeks to guarantee better cooperation between security and judicial services. The quick emergence of loopholes in the judicial treatment of cybercrime urged several actors to take actions. A few projects have emerged in Europe and the focus will be on two of them: CyberSouth and ENISA (The European Union Agency for cybersecurity). CyberSouth (Cooperation on cybercrime in the Southern Neighbourhood Region) project is part of a dual approach: on the first hand, the ambition of the Council of Europe which aims to enforce the Budapest Convention through this project; and on the second hand, the desire of the European Union (EU) to include cybercrime and its judicial treatment in respect to the rule of law as part of the Neighborhood Policy. The priority zones of CyberSouth are Algeria, Jordan, Lebanon, Morocco, and Tunisia. CyberSouth was created in a context of weak cyber security with ineffective repressive policy regarding cybercrime, especially coming from some States. The issue lies with the way of transmitting proof of a cybercriminal act for a fair judicialization. Indeed, without this proof, the risk is much greater for a judicialization without proof on the part of the states lacking effective means of cyber-police, which constitutes a considerable threat to the rule of law. The European Union has also subscribed to this need for effective cooperation between European judicial services and their partners in the South,

which are for example often weaker in providing evidence. The EU saw: cybercrime and the inability of a security and judicial response from certain States certainly threatens national security but also tends to weaken the rule of law through an inappropriate response from a legal point of view. Thus, it has brought CyberSouth to the heart of its Neighborhood Policy and the aim of which is to "support and promote stability, security and prosperity in its immediate neighborhood." Therefore, the genesis of the CyberSouth project is to ensure within countries of the South an equally strong and fair repression of cybercriminal acts that comes as close as possible to the European model. In fact, the CyberSouth project is funded up to 5 million euros and has since its launch in 2017, materialized by several tangible results:

- "Enhanced criminal law framework" in cyber matters
- Creation of a "specialized police and prosecution services and strengthening of interservice cooperation for a sustainable approach".
- "Standardization of the training of members of the judicial system in the fight against cybercrime and the processing of electronic evidence"
- "The criminal justice authorities have better skills and better tools for more effective international cooperation in cybercrime and electronic evidence".
- The priority strategies in cybercrime and electronic evidence are identified.

CyberSouth is not the only project which has been implemented in Europe in order to fight cyber criminality. Indeed, the European Union is very motivated to solve this issue and has, in this purpose, created the European Union Agency for Cybersecurity (or ENISA). This agency was established in 2004 and it has been strengthened by the EU Cybersecurity Act which granted it a permanent mandate. This act also increased ENISA's operational cooperation at the Union's level. making it easier to support states needing assistance in dealing with cybersecurity issues. It is part of Cyber Europe which is a series of pan-European large-scale cyber security exercises aimed at testing crisis management capabilities, cybersecurity, and business continuity. This agency is helping European countries through information sharing, capacity building and awareness raising. Its final goal is to "keep Europe's society and citizens digitally secure". Indeed, the world is becoming everyday more and more connected and the threat to internal security of the European Union grows every day. This year with the COVID-19 pandemic, the need for more security in the digital world has been highlighted. Indeed, because of several lockdowns that the countries are implementing, people rely on their online presence more and more of their life depends on cybersecurity and the protection of their data. Cybercriminals have taken advantage of

	this situation, particularly in the field of e-commerce and e-payments as these have significantly increased this year, making them profitable targets. The healthcare system has also been a preferred target of cyber criminals. ENISA's missions include: - Empowering communities: ENISA plays a key role in stimulating cooperation between the Member States and the EU institutions and agencies in cybersecurity. It tries to ensure efficient common efforts in this field. - Cybersecurity policy: ENISA thinks that cybersecurity must not be restricted to a specialist community of technical cyber experts. Cybersecurity must then be included across all domains of EU policy, leading to a coherent approach. - Operational cooperation: the cyber criminals know no borders when they are attacking, this is why ENISA promotes a more efficient cooperation between member states. This cooperation allows a faster and more effective response - Capacity building: the frequency and sophistication of cyber attacks constantly increases nowadays. Therefore ENISA is participating in the modernization of the response system: building competences and acquiring the right material.
-Envisaged format for the presentation (ppt,video,other)	Video

(*)**to be sent by December 10th to** : mariadinatozzi@gmail.com; m.camiade@iec.cat; robert.botteghi@univ-cotedazur.fr