

**Country: Italy**

**Committee: United Nations General Assembly(UNGA)**

**Agenda: Advancing Responsible State Behavior in Cyberspace in the**

 **Context of International Security**

**Delegate: Varun Sibi A P**

 The aims are to improve awareness of cyber security management in the various national settings, support nations in enhancing their own cyber security governance, encourage the spread of best practice, and contribute to the development of interagency and international cooperation. Primarily focusing on NATO nations that are Sponsoring Nations to the CCDCOE, each country report outlines the division of cyber security roles and responsibilities between agencies, describes their mandates, tasks, and competences and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines national cyber security strategy objectives to clarify the context for the organisational approach in a particular nation. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations including Italy providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. At the heart of the Centre is a diverse group of international experts from military, governmental, the cyber threat has in fact created a time-space collapse that has essentially destroyed the threat management models as conceived so far. The enemy can be anywhere, at no more than a hundred milliseconds away from you; a single enemy, with even only an average cyber capability, can simultaneously attack thousands of a Italy’s strategic assets. This is why we need a new way of interpreting national security, which should also consider the cyber protection of the country by an operational coordination plan that must be flexible, adaptable and have a very short chain of command, i.e., fast in the response. Raising the Italy’s level of security and resilience necessarily requires an increase in the level of security and resilience of each of the components of the overall framework. The closer you are to the middle of the picture, the more you need to increase response coordination and speed. The sector with inadequate defense becomes, in fact, the weak link of the entire Italy system. The levels of security are peculiar to the specific asset. While, for example, citizens are required to maintain an adequate form of cyber-hygiene, the CISR is required to have an extremely sophisticated and articulated security infrastructure with rapid response times. It is advisable to immediately highlight how, in order to minimize the consequences of an attack, a sequence of operations must be activated in the shortest possible time by the NSC and by its operational players as stated in the National Plan. These actions include, for example, the detection by the target asset of the ongoing attack, the notification of the attack to the NSC, the academic and industrial background assessment done of the threat entity, the identification of potentially attacked assets and actions to be taken, their communication by the NSC to the assets involved, and the application of appropriate countermeasures by these assets. To deal with the threat caused by the collapse of the cyberspace, it is necessary to reduce the transit times of relevant information to the point where it can be handled appropriately, bringing to the heart of the system only those events that threaten national security in terms of the economic, political and scientific interests of the country. A sort of nervous system of the Italian platform overlying the assets This nervous system is formed by the constituencies of NSC operational players and by the Centre of Competence ..