Cyber-security: Geopolitics as Usual

In the contemporary international system, the emergence of cyberspace has not merely introduced a new medium for communication but has fundamentally extended the theatre of geopolitical competition. Within the **Security and Technology** Master's program at the National University of Political Studies and Public Administration, the course **Cyber-security: Geopolitics as Usual** offers a sophisticated exploration of this digital frontier. The discipline approaches the cyber dimension as a distinct and critical level of analysis in international relations. It posits that while the technology is novel, the underlying struggle for power, influence, and security remains a fundamental constant—a phenomenon aptly described as "geopolitics as usual."

The academic framework of the course is designed to dismantle the silos between technical capability and political strategy. Students are tasked with the rigorous mastery of a specialized lexicon, ensuring the precise application of concepts such as cyber-defence, cyber-warfare, cyber-espionage, and cyber-resilience. This conceptual clarity is essential for identifying the main actors in the cyber realm and for understanding how digital vulnerabilities influence security architectures at the individual, national, and international levels. By analysing the "uncontrolled" nature of cyberspace, the curriculum challenges students to consider the tension between the inherent freedom of the internet and the state's obligation to provide security and maintain sovereignty.

A central pillar of the syllabus is the comparative analysis of national and institutional strategic approaches. The course provides a deep dive into the diverging cyber doctrines of global powers, including the United States of America, Russia, China, and Israel alongside the collective security frameworks of NATO and the European Union. This comparative lens allows students to discern how foreign policy is projected into the digital sphere and how regional security is reshaped by cyber capabilities. Furthermore, the inclusion of a specific focus on Romania's national approach ensures that students can contextualize these global trends within their own immediate strategic environment.

The didactic methodology transitions from theoretical inquiry to practical simulation, bridging the gap between academic research and professional application. Through UN-style model simulations and interactive debates, students engage with complex case studies regarding the evolution of the threat environment and the ethics of digital offense versus defence. These exercises are designed to strengthen analysis and synthesis skills, preparing students to formulate high-level policy recommendations in a multidisciplinary context.

Ultimately, this course prepares future experts to navigate a world where online security and physical freedom are in constant negotiation. The expertise gained here is directly applicable to careers in international organizations, government defence sectors, and strategic consultancy within the private industry. By the conclusion of the semester, students will have developed a critical perspective on the interdependencies of the digital world, positioning them to manage the risks and vulnerabilities of a global landscape where the next geopolitical shift is likely to be initiated by a line of code.