Rezumat în limba engleză

From 2015 to the present, my professional activity has represented an integration of three complementary perspectives: teaching and learning, research, and professional engagement, with the assumed objective of building a prestigious academic career grounded in a solid scientific foundation.

The habilitation thesis reflects my academic research activity and professional experience as a university lecturer and seeks to demonstrate my competence to supervise doctoral research in the field of international relations. The habilitation thesis is structured into two major chapters, which aim to capture, as accurately as possible, my academic profile.

The first chapter—*Professional Milestones and Scientific Contributions*—focuses on presenting the main outcomes of my professional trajectory, highlighting relevant moments in my academic activity. It continues with an overview of my professional development during my doctoral studies (2012–2015), my participation in advanced training courses at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, and concludes with my scientific evolution following the attainment of the PhD degree. This chapter also briefly presents the main research projects in which I have participated, their outcomes—materialized in scientific articles and/or books, presentations at national and international conferences—as well as extracurricular activities (such as membership in scientific or editorial boards of journals indexed in international databases, activities as a trainer, or as a coordinator of externally funded research projects). In my view, all these elements demonstrate innovation, continuity, and coherence in my scientific endeavors, judiciously integrating an interdisciplinary approach to international security, with a particular emphasis on cybersecurity, while also highlighting my ability to work within and coordinate research teams.

In the final part of this chapter, I sought to emphasize the importance of an interdisciplinary approach to the study of cybersecurity. Evidently, my ontological, epistemological, and methodological choices are situated within neorealism and the Copenhagen School, not so much for the purpose of establishing causal relationships, but rather for examining their influence on changes in security dynamics at the level of public policies related to cybersecurity.

The evolution of societies, the technological revolution, and new types of threats to humanity bring to the forefront issues that were previously addressed strictly at the domestic or technological level, thereby redefining the role of states within the international security

architecture. Consequently, we are witnessing a possible paradigm shift in international relations, which at the strategic level had been based on the nuclear strategy of mutually assured destruction, and which the specialized literature has attempted to encompass under the umbrella of cybersecurity. The analysis of these changes requires an interdisciplinary approach, as the traditional field of study limited to political science, international relations, and public international law proves insufficient. For this reason, in my research I have sought to adopt an interdisciplinary perspective, drawing on other fields such as strategic studies, security studies, technology studies, and strategic decision-making processes, in order to address issues related to disarmament, arms control, dual-use goods, and communication, with an emphasis on new communication environments. Another interesting and relatively underexplored research direction concerns the need to theorize cybersecurity. Although there is literature addressing the cyber domain, there is an almost complete absence of a meta-theory of cybersecurity capable of integrating all relevant concepts into a single coherent set of relationships. Such an endeavor is possible only through a collective effort involving academic theorists and career diplomats. The starting point in developing a meta-theory should be the clarification of the relationship between diplomacy and theories of international relations. A legitimate question thus arises in the academic environment: is cybersecurity an autonomous concept, or must it rely on the criteria of the Copenhagen School, or be viewed exclusively from a technological perspective in order to explain developments in the international environment? If cybersecurity is understood as being subsumed within international relations (a position that holds if we accept that states are the only relevant actors), then the theoretical framework of international relations is sufficient. However, what if cybersecurity is broader than international relations? I have argued that actions and gestures undertaken by non-state entities in their attempts to interact on the global stage for the purpose of international recognition can also be subsumed under cybersecurity.

As previously noted, I have drawn on my background in management to highlight a possible missing link in attempts to theorize cybersecurity, namely the insufficient research into this field and into the manner in which states implement foreign policy. Cyberspace has become an integral component of nearly every segment of a state's national critical infrastructure, whether civilian—such as hospitals—or military—such as nuclear power plants—thereby transforming their owners and operators into both potential security providers and potential security vulnerabilities. At the same time, the degree of economic interdependence is so high that it is no longer possible to analyze one's own security without taking into account the security or insecurity of others. Moreover, the number of actors

involved has increased significantly. Furthermore, cyberattacks are considerably less costly than conventional attacks, which has led to large-scale attacks with losses estimated in the billions. At the same time, the heterogeneity of actors involved in cyberspace generates the need for clear regulations, which the international community currently lacks. I have sought to argue the importance of adopting an interdisciplinary research perspective on cyberspace in the effort to theorize cybersecurity and the necessity of drawing on the analytical tools of other disciplines, such as management, in order to demonstrate how technology must be integrated into the internal and international processes of states.

At present, technological development generates new threats and risks to national and international security agendas, which states must address in cyberspace. Given the multitude of actors involved, motivations, strategies, and types of attacks, the classical way of conceptualizing security, war, and deterrence is no longer functional. In this context, the majority of states have developed their own national cybersecurity strategies designed to highlight their approaches to cyberspace (in the case of the European Union, this process is mandatory for all Member States through the NIS Directive). This evolution has revealed heterogeneity not only among traditionally opposing actors such as the Russian Federation, China, and Western states, but also among allies, namely NATO and EU Member States. From a legal perspective, at the international level, no significant qualitative progress has been achieved, as no new binding regulations have been developed. The only relevant regional normative actor in this field appears to be the European Union; however, given its limited competences in the areas of defense and military (hard) security, its actions have had a limited international impact in terms of altering state behavior. Moreover, the Tallinn Manual represents the only comprehensive resource addressing questions of who, what, when, how, and why cyberwar can or cannot occur, yet its legitimacy is recognized predominantly by Western societies. Additionally, it constitutes merely one interpretation of existing international law, rather than the law itself. At the same time, the perspective according to which the state is the sole provider of security or insecurity has become obsolete, given current security dynamics in which critical infrastructure is overwhelmingly owned and operated by private companies, and the costs associated with developing and conducting a cyberattack are relatively low, thus allowing for the involvement of individuals as well. Under these circumstances, I have aimed to develop a comprehensive perspective on current security dynamics, taking into account the transformations generated by the cybersecurity domain and the ways in which states and international organizations can manage these emerging threats in a sustainable manner. The second chapter presents the plan for my academic career, the main

lines of development of my research and teaching activities, new publication plans, and possible future doctoral research topics. Within this chapter, I detail the results of my academic research, the research directions I intend to pursue in the field of cybersecurity, future projects, and the establishment of a center of excellence in public policy in the area of cybersecurity. These new research directions may have direct applicability in the academic environment by enabling an improved learning experience for students, while also proving useful for professionals in international relations by offering insights into a possible rethinking of how national and international security strategies are developed (Costea, 2026).

I also present a publication project released in 2026, namely the single-authored book *Cyber Deterrence and State Response in the Age of Technology: Strategies and Challenges*. The book was published by Springer and includes, in addition to a necessary revision of some of the topics addressed, an analysis informed by developments on the international stage from the 1990s to the present.

In the final part of the chapter, I propose several doctoral research topics that fall within my ontological, epistemological, and methodological preferences.