AUTHOR

Tatiana A. Romanova — PhD (Political Science), Associate Professor at the Saint-Petersburg State University (e-mail:t.romanova@spbu.ru, romanova@mail.sir.edu); *Alyona N. Malova* — PhD Candidate at the Saint-Petersburg State University (e-mail: alenamalova5@gmail.com).

TITLE

THE EUROPEAN UNION CYBERSECURITY POLICY: OPERATIONALIZATION OF THE RESILIENCE CONCEPT

SUMMARY

The unique nature of cyberspace, characterized by interdependence between material and social objects as well as the complexity of its structures, urges leading actors of world politics to seek new strategies of organizing their activities within this area. In the European Union, cybersecurity issues are debated on the basis of the resilience category. In this context the latter is understood as a system's ability to adjust to new challenges, flexibly respond to threats, and successfully recover after blows. Using a discourse analysis approach the authors examine the genesis of the resilience discourse and the logic of its development in the EU cybersecurity policy, reveal nuances of how this category is interpreted in official documents as well as point out difficulties regarding practical application of this category.

The authors trace a gradual evolution of the EU approach towards cybersecurity from the well-established definitions of cyberspace to the ecosystem terms and concepts, which are particularly relevant to the resilience-based concept of cybersecurity. Within this approach, the Internet is considered not as a static object but as a complex heterogeneous system where a state of security is inextricably linked to a state of insecurity. There is no single and coherent definition of resilience in the EU official documents yet. Nevertheless, it is stressed that one can see a gradual transformation of the official discourse from purely technical definitions to inclusion of a wider range of socio-political factors. However, the EU official discourse on this issue remains highly controversial. This refers, for instance, to the lack of a unified understanding of the 'cyberresilience' and 'cybersecurity' concepts. The authors highlight a tendency towards increasing securitization of the cybersphere in the EU cybersecurity discourse, which might lead to the narrowing of the concept of 'cyberresilience' and its transformation into a common euphemism. At the same time the authors conclude that the EU itself is not interested in oversecuritization of the cybersphere, and thus the EU cybersecurity policy will eventually evolve towards resilience-based approaches.

KEYWORDS

the European Union, resilience, cybersecurity, cyberthreats, cyberresilience, cyberecosystem, securitization, Critical Information Infrastructure, European Union Agency for Network and Information Security, ENISA.

ACKNOWLEDGEMENTS	The reported study was funded by the Russian Science Foundation according to the research project 17-18-01110.