

CHARLES UNIVERSITY
FACULTY OF SOCIAL SCIENCES
Master of International Security Systems

Anastasiya Neskromna/Rieger

**Impact of COVID 19 on Security Policies of States
in the Area of Cyber Security**

Abstract

Prague 2022

Author: Ms. Anastasiya Neskromna/Rieger

Supervisor: prof. David Erkomashvile, Ph.D.

Academic Year: 2021/2022

Abstract

The SARS-Cov-19 or in different wording the global Covid pandemic outburst have created an unprecedented scenario for various organizations, agencies and structures.

The COVID-19 pandemic in 2020 has become an extraordinary and shocking event for the world community and the global economy. On the part of the authorities, the COVID-19 pandemic is accompanied by sometimes harsh and ambiguous decisions, the consequences of which are felt by people in many countries of the world: movement between countries was stopped, businesses and enterprises were closed, the restriction was created, those who were sick or at risk of infection were isolated. There was also no possible assumption regarding how long such a mode of life will last. Many factors as a consequential chain of reactions from the pandemic in the aggregate have created a pleasant environment for altering and modifying the cybercrime landscape.

This work aims to analyze the factorial presence of modification in the sphere of cybercrime, cybersecurity, and governmental responses. Based on the results of the analytical assessment, it is highly recommended that different governmental structures should collaborate more on inner domestic collaborative levels among units and on external international levels among multiple governments. The creation of unified international legislation to protect entities and individuals is also highly recommended.

The initial purpose of these work is to investigate and identify the prospects of perpetual correlation including direct and indirect opportunities and features of SARS-COV-19 global pandemic outburst and the consequential effects firstly, on the cyber security sector, including current state, developmental stage in process, and future prospects of revitalizing the field, upcoming prospects; secondly, the alteration of cybercrime landscape, the new features and strategical decision of modernization and hybridization techniques, incorporation of cybercrime activities into governmental structures as a part of the strategical superiority and as a new stage of warfare; Thirdly, the responses of international communities and governmental responses, the possibilities of securitization against this types of threat, the legislative incorporation into the systematical approach, the prospects of multi-government collaborative relationship for the purposes to the cyber threat preventive measures.