On September 7, 2020, a representative of the Personal Data Protection Agency participated in the Zagreb Security Forum entitled "Hybrid threats and wars in the 21st century - how to make society and infrastructure resilient."

The focus of this year's Forum, which is the leading annual meeting of foreign and Croatian experts on information security and critical infrastructure protection in Southeast Europe, was to identify and confront complex forms of hybrid threats in order to organize effective and preventive protection of fundamental social values, democratic system and critical infrastructure, with an emphasis on energy and cyber infrastructure.

The gathered experts pointed out that countries are exposed to hybrid threats on a daily basis, and hybrid attackers exploit existing and create new vulnerabilities / divisions of society, democratic structures and institutions using political, economic, military, civilian, security, intelligence, energy, media, information and communication systems. and resources.

Over the last decade, a number of state and non-state actors have developed digital marketing techniques, enhanced by cyber and psychological operations they use to change political reality, make profits, and shape public knowledge.

Such techniques often include hacker attacks, propaganda and disinformation, and are of particular concern in the context of the COVID-19 pandemic, which could serve as a testing ground for hybrid action to jeopardize state security systems and create an alternative worldview designed to undermine democratic values. . It is vital that this global health crisis does not turn into a global security crisis.

Fake news and messages that cause polarization in society are very easy to spread in the digital ecosystem, especially through social media, and the goal is to encourage individuals to react and engage. This is most easily achieved through sensationalist messages and misinformation that provoke strong emotions in people such as fear, anger and hatred.

Dissemination of misinformation implies the intentional creation and dissemination of false and / or manipulated information with the intention of deceiving and / or misleading. Disinformation tends to deepen divisions within and between countries, and undermine people's trust in national governments.

Disinformation campaigns conducted by state and non-state actors aim to create distrust in democratic institutions and present authoritarian regimes more successful in dealing with the health crisis. They also pose a risk because they undermine key public health recommendations.

Furthermore, hybrid operations involving disinformation campaigns pose an increasing threat to democratic and transparent electoral processes, as we have witnessed in the Cambridge Analytica case.

In today’s digital age when many business models and processes are based on collecting large amounts of data, with the goal of predicting human behavior and making a profit, voter votes are often sought in an unfair, illegal and manipulative way. Unfortunately, it was only a matter of time before different state and non-state actors realized that they could use this non-transparent system to achieve their political goals.

Large amounts of personal data that we often carelessly and excessively share on social networks pose a great danger to individuals, society, national and European institutions. The personal data of hybrid attackers can be misused to manipulate security processes, thereby undermining the foundations of our democratic system and undermining trust in state institutions. Forum participants concluded that a comprehensive understanding of the information environment, especially misinformation, is key to enabling a credible response to these threats.

All the conflicts that await us in the future will use hybrid attacks on key infrastructure, and the latter will be particularly exposed to identity, that is, everything that makes a particular community a cohesive group.

To protect against hybrid threats, a joint and coordinated response from all stakeholders is needed: from national governments, regulators, international organizations, civil society organizations, private companies, the media and the individual. It is up to individuals to develop critical thinking, and it is up to states and organizations to develop early detection and response systems.