It is a great honour for me to have this opportunity to deliver this presentation.

The exponential use of internet services for day-to-day communications and activities has led law enforcement authorities to increasingly rely on the access to and collection of electronically stored data for the investigation of crimes and prosecution of perpetrators. Information transmitted in digital form and stored by private service providers in different countries are considered to be valuable and often indispensable, probative sources. Granting law enforcement agencies the possibility to promptly gather different types of electronic data across borders is considered crucial not only for the countering of cybercrime, but also for the investigation and prosecution of criminal offences in the offline world.

The success of many cybercrime or other investigations depends on the accessibility of electronic evidence stored abroad. However, as a State has sovereignty, so it has territorial boundaries. Cybercrime ignores frontiers, since cyberspace is a unique realm. It has no boundaries, and it is difficult to say which part of it falls under a state sovereignty and which part does not. And what is more, cyberspace has no unified law to govern it – not even a unified legal definition. However, the need to define and govern cyberspace is still growing.

History has witnessed such situations. When maritime trade and navigation became an issue, legal rules were born, as early as in the ancient Roman times, then Hugo Grotius lay the foundations of the modern Law of the Sea, which eventually developed to be a body of laws that reliably govern jurisdictional, navigation, fishing and liability issues. When space exploration became a reality, international space law was created. Cyberspace resembles the seas and the outer space, although there are differences too. No nation may claim sovereignty over any part of space, all nations have equal rights to explore and research it (r*es communis omnium usus*). Cyberspace, on the other hand, is a virtual field that has data entry and exit points that are mostly in a state's territory. Perhaps, in the near future, nations might be able to create an international cyberspace law, accepted by all sovereign states and international organizations, governing jurisdiction and other issues that arise

from the unique features of cyberspace. Such law must include rules that would make obtaining electronic evidence easy and quick as well as safe and legal.

The Council of Europe has been the home of many positive and forward-looking initiatives. Let me draw your attention to three of them, all of them are outstanding in their nature and importance.

In 2006, the Consultative Council of European Prosecutors (CCPE) held its first meeting in Moscow. The CCPE has had an undeniable influence on the work and role of prosecutors throughout Europe.

In the fifteen years since its establishment in 2006, the Consultative Council of European Prosecutors has been active not only in the criminal field but also in the non-criminal field because in some Member States of the Council of Europe the prosecution services have some tasks and functions outside the criminal law field. The Opinion Nr. 3 on *"The role of Prosecution Services outside the criminal law field*" adopted by the CCPE in 2008 emphasizes and underlines the protection of the environment, the consumers and the social rights of citizens. The standards of the Opinion aim to provide the efficiency in this field and to ensure that the protection is in line with the rule of law.

As in the whole work of the Council, we can thank to the colleagues from Russia for the significant and fruitful contribution in drafting this Opinion.

The Council of Europe's 2001 Cybercrime Convention – commonly known as the Budapest Convention – is, in my opinion, another important initiation, moreover, it can be considered as a good first step toward the above mentioned legal base for a better and more effective cyberspace law.

Criminality in cyberspace is rapidly evolving, and the law enforcement together with criminal jurisdiction must not lag behind. Even a modern and effective body of laws concerning cyberspace

must be agreed upon and accepted by sovereign states. I am convinced that such "international cyberspace law" will open up a wide range of possibilities in obtaining evidence in criminal procedures. This is what I expect in the future, and my expectations are based on the Budapest initiative.

Until then, authorities have to rely on the existing forms of judicial cooperation mechanisms such as mutual legal assistance or, within the EU, mutual recognition, as well as on the direct cooperation of service providers, or on direct access to obtain information. All three channels raise different types of issues affecting the success of investigations resulting in abandoned and unsuccessful cases and, ultimately, in a less effective administration of criminal justice.

International cooperation depends on harmonized national substantive laws, which criminalize cybercrime, and national procedural laws that set the rules of evidence and criminal procedure. It can also be facilitated by harmonizing, wherever needed, bilateral, regional, and multilateral instruments on cybercrime. However, even with harmonized laws, international cooperation in cybercrime investigations can be challenging. What complicates matters is the lack of timely collection, preservation, and the sharing of digital evidence between countries through formal cooperative mechanisms.

Informal mechanisms for international cooperation, such as the sharing of information between law enforcement agencies to obtain legal and technical advice and assistance in cybercrime cases as well as to request the collection of digital evidence are also of great importance.

Even with the formal and informal international cooperation mechanisms in place, challenges arise in the identification and collection of digital evidence from cloud storage and other service providers. The problem with cloud computing is that it is difficult to know where data is stored. Without this knowledge, the relevant jurisdiction to which a cooperation request should be sent to obtain digital evidence cannot be identified.

Cloud data can be fragmented and stored across multiple locations and multiple countries.

Despite its legal basis being highly controversial, law enforcement authorities are increasingly approaching service providers outside the mutual legal assistance model. As its name indicates, under this direct cooperation model, investigators directly contact service providers without any intervention of the authorities of the country to which the request is sent. There is currently no common position about the lawfulness of direct cooperation, which is a circumstance that came about for two main reasons. First, the differences among member states' regulation of domestic and foreign service providers. Second, due to the absence of rules on whether requests issued directly to a service provider in another country are voluntary or mandatory for the service provider being addressed.

Over and above what has been said, international cooperation depends on states' abilities to process requests for evidence in a manner that ensures the admissibility of evidence in court. To achieve this, qualified cybercrime professionals are needed to ensure that evidence is obtained according to national rules of evidence and criminal procedure. Sufficient funding, qualified personnel, technical equipment and tools to conduct cybercrime investigations, universal digital forensics and evidence standards and protocols, which ensure the admissibility of digital evidence in the national courts of cooperating countries, are crucial, because only a multifaceted approach targeting the above-mentioned areas could improve international cooperation on cybercrime and cyber-related matters.

I am convinced, that the need arising from all of these will lead to a clear, reliable, 21st century legal background, a modern legal base upon which criminal justice can raise an even more effective combat against cybercriminality.