

**Programme of the Third International Scientific Conference**  
***"The Multidimensionality of Cybersecurity.***  
***New dimensions of digital crime: law, technology, society"***  
**16-17 April 2026**

**Helena Chodkowska University of Technology and Economics**  
**135 Jutrzenki Street**  
**02-231 Warsaw**

**16 April 2026**

**13:00 – 14:00 REGISTRATION OF PARTICIPANTS**

**14:00 – WELCOME BY DR JUSTYNA ŻYLIŃSKA, Rector of the University**

**2:10 p.m. – INAUGURAL LECTURE,**  
**DR KRZYSZTOF GAWKOWSKI,**  
**Deputy Prime Minister, Minister of Digital Affairs**

**14:30 – 19:00 – FIRST PANEL: ORGANISATIONAL AND LEGAL SYSTEM IN THE FACE OF  
CYBER THREATS – CHALLENGES AND SOLUTIONS**

**COFFEE BREAKS: 15:30 – 15:45 and 17:30 – 17:45**

Legal and organisational systems are not keeping pace with the dynamic development of technology. A significant proportion of digital crimes are cross-border in nature, which creates difficulties in determining jurisdiction, harmonising legal regulations and effectively prosecuting perpetrators. At the same time, the development of digital documents and electronic information flow creates new opportunities for cybercriminals, who are increasingly attacking both IT systems and traditional data carriers. This phenomenon includes, among other things, the falsification of electronic documents, identity theft, data manipulation and impersonation of authorised persons in order to gain access to sensitive information.

As a result, it is necessary to create and update regulations – both at national and international level – that take into account the specific nature of cyberspace, the protection of human rights and privacy, as well as the need for close cooperation between states, international organisations and the private sector.

**7.30 p.m. – GALA DINNER**

17 April 2026

**9:00 a.m. – 1:00 p.m. PANEL TWO: THE TECHNOLOGICAL DIMENSION OF CYBERCRIME**

**COFFEE BREAK: 10:30 a.m. – 10:45 a.m.**

Modern technologies today play a dual role in the field of cybersecurity – on the one hand, they are used to commit crimes, and on the other, they are key tools for detecting and combating them.

The panel will discuss key technological aspects of cybercrime, including methods of securing IT systems, the use of cryptography, zero trust solutions, and the use of artificial intelligence and machine learning to detect threats.

Particular attention will be paid to assessing the effectiveness of modern analytical and predictive tools and identifying new and emerging risks, such as deepfakes, botnets, exploit kits and the dark web, which can lead to data manipulation, disinformation and breaches of the security of digital documents and IT systems.

**13:00 – LUNCH**

**14:00 – 15:30 PANEL THREE: THE SOCIAL DIMENSION OF CYBERSECURITY. HATE SPEECH**

**COFFEE BREAK: 3:30 p.m. – 3:45 p.m.**

The internet has become a space for both open dialogue and growing hate speech, which has serious social, psychological and legal consequences. The panel will discuss the scale of this phenomenon online, the legal and technological mechanisms available to limit it, and effective ways to counteract it. Particular attention will be paid to the role of online platforms, the media and user responsibility in creating a safe and responsible *online* space. The discussion will focus on practical solutions, good practices and actions that can help reduce online hate speech.

The panel will be set in the broader context of cybersecurity, which is not only a matter of technology and regulation, but above all of awareness, education and user responsibility. Experts will discuss the impact of cyber threats on society, including the problems of disinformation, privacy protection and digital exclusion.

**15:45 – 18:00 PANEL FOUR: INTERNATIONAL COOPERATION IN THE FIELD OF CYBERSECURITY -**

In an era of dynamic global digitalisation and growing dependence on IT systems, cyber threats are becoming increasingly complex and cross-border. Attacks on critical infrastructure, disinformation campaigns, data leaks and cybercrime are not limited to national borders, which necessitates a new quality of international cooperation. As a result, states, organisations and institutions must face legal, technical and operational challenges that require coordinated action and a coherent regulatory framework.

The panel will focus on international cooperation in the field of cybersecurity, applicable regulations and mechanisms for responding to cross-border cyber incidents. Experts will discuss issues of digital sovereignty, the responsibility of states and private entities, and the effectiveness of the current legal framework. The discussion will focus on practical solutions and directions for the development of cybersecurity policy at the international level.