Abstract of the project:

In modern society, information and communication texhnologies have penetrated deeply and have become the basis of all activities in the economy, administration, public and private life. Digital infrastructures become supportive environment of a major and critical factor for the management and proper functioning of all resources and systems of national importance, the development of competitive and innovative economy and transparent management of a modern democratic civil society. At the same time, the growing and irreversible dependence on digital basic functions and activities of the society raises significant new risks and threats. Therefore, to achieve a sufficiently high level of network and information security is critical for reliable and effective functioning of these activities. This occurs in so-called "Critical infrastructure", providing vital functions of the economy and society (energy, transport, banking, healthcare, security and defense, etc.).

On the other hand, in parallel with the positive developments of the information society rapidly appears and spread worldwide and its negatives - global cyber-crime. According to most analysts, it already notes the fifth generation, characterized by automation development and dissemination of tools to attack and integration if a few sets of tools that perform different functions. One of the peculiarities of the fifth generation is so-called " Advanced Persistent Threats (APT)" - targeted attacks against specific organizations by certain, well-coordinated cyber-criminals. In the community of experts, APT most often refers to sophisticated attacks aimed at governments and corporations. APT is often used by public authorities or their agents, as well as terrorist and separatist political groups.

Risks and threats in cyberspace are difficult to define, because of the complexity of determining the source of impact, objectives and motives, the rapid escalation of the threat and difficult foreseeable prospects, complexity and intensity of modern communication and information processes, the dynamics of logical and physical connections and the uncertainty of the process. Among the most serious destructive effects are those of a hybrid character - a combination of cyber-attack and physical attack, cyber-attack aimed at critical kinetic process, cyber-attack during a natural disaster or malfunction in critical systems. Equally affected by cyber incidents random or targeted cyber-attacks are public and private sector and society in Bulgaria.

Connectivity and dependence in cyberspace allows security breaches or failure of a communications and information system from a sector lead to a cascading effect and failure in others, again with serious consequences and possible harm to vital services. Response to such incidents requires coordinated actions and preventive measures to minimize opportunities develop into crises, and adequate follow-up, leading to timely restore the functioning of the systems.

In general, threats can be grouped conditionally of three upgrading levels:

- "Known known" - known weaknesses, threats and breaches associated with major "triad" of information security (CIA - confidentiality, integrity, availability);
- "Known unknowns" - combined threats related to information security, a variety of APT, attacks at the reputation of organizations and individuals, disinformation campaigns and other unpredictable consequences of the mass transfer of our activities in cyberspace, CIA breakthroughs in particularly large scale (national, regional and global) requiring extensive and systematic application of CIA for all assets in the digital ecosystem
- "Unknown unknowns" - unpredictable, unexpected threats in cyberspace dynamically changing risks and complex effects with unpredictable consequences that require flexibility and sustainability of the systems, organization and processes, and relevant requirements in the development and commercialization - the main features of state cyber sustainability.

In these conditions the overwhelming amount experts are united around the idea, that traditional methods of protection are already less productive and its needed a qualitative

approach to new tools for the implementation of network and information security.
One of those priority areas of this approach is the widespread use of intelligent methods for analysis of the exchanged information, flows in networks, the sources of threats and planning effective measures for impact, including proactive (attacking the main sources of threat, such as control centers of "bot-net" and so on.).
World practice has noted a significant number of different applications of "artificial intelligence" in computer security. So far without doing attempts for a comprehensive classification, we can divide those applications in two main directions:
A. Conditionally called "distributed" or "network" methods:
A1. Multi-agent systems of intelligent agents;
A2. Neural networks;
A3. Artificial immune systems, genetic algorithms, and so on;
B. Conditionally called "compact" methods:
B1. Systems of Machine Learning (Machine Learning), including associative methods, inductive logic programming, Bayesian classification and so on.
B2. Algorithms for pattern recognition;
B3. Expert systems;
B4. Fuzzy logic and so on.
The project aims to systematize, analyze and assess the various uses of "artificial intelligence" in computer security. To choose the most promising national practice methods. To make recommendations for their use.
It should be noted that according to literature applications of artificial intelligence is used in three main actions related to computer security:

- Detection;
- eliminate the consequences (repair);
- defense (defense) - passive and active.

This project is expected to pay special attention to the first act. It will attempt to justify and formulate elements of the new concept of "Cyber Intelligence".
Preliminary analysis of the methods of "artificial intelligence" used in systems for Network and Information Security show that most of them have both advantages and disadvantages. One of the main objectives of the project proposal is once held in-depth analysis, accompanied by experimental study of the most promising methods to attempt to improve the positive aspects and avoid disadvantages - either by modifying the selected method or hybridization a few selected method.

Coordinator of the research team		
Assoc. Prof. Ph.D. Eng. Roumen Ivanov Trifonov		
Team members:		
Prof. Ph.D. Eng. Ognian Nakov Nakov Prof. Ph.D. Eng. Daniela Asenova Gotseva Prof. Ph.D. Eng. Hristo Angelov Hristov -retiree Prof. Ph.D. Eng. Milena Kirilova Lazarova-Mitzeva Assoc. Prof. Ph.D. Eng. Plamen Ivanov Vatchkov - retiree Assoc.Prof. Ph.D. Eng. Slavcho Aleksandrov Manolov - retiree Assoc. Prof. Ph. D. Radoslav Dakov Yoshinov –Lab. of Telematics, BAS Assoc.Prof. Ph.D. Eng. George Ilinchev Popov Assoc.Prof. Ph.D. Eng. Adelina Plamenova Aleksieva-Petrova Assist. Prof. Eng. Galia Veselinova Pavlova MSc. Eng. Georgi Roumenov Tsochev Eng. Momchil Mariyanov Petkov	PS PS ST	