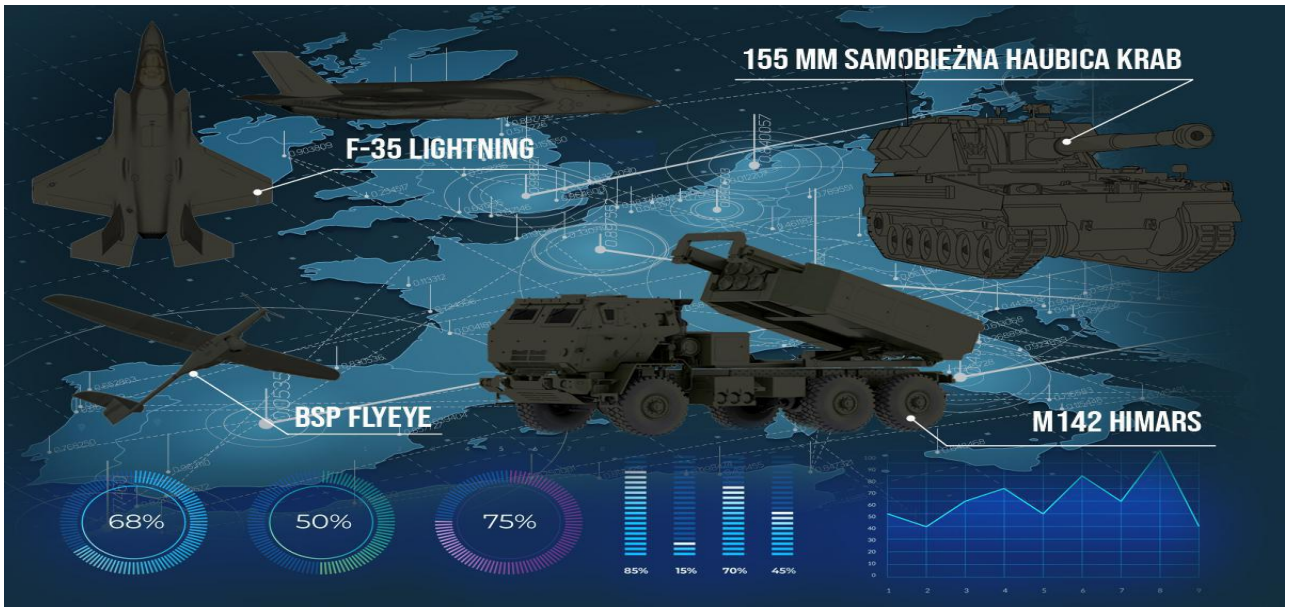
25 April 2022

Safe Cyberspace



At the beginning of the 2020s, one could notice a trend in the development of information society which is closely linked to the development of IT. The increased use of these technologies coincided with the time of the COVID-19 pandemic and the spread of SARS-CoV-2. The growth in the infection rate, imposition of restrictions, lockdown of individuals and societies, introduction of changes in work organization (remote work, hybrid work) both in the physical dimension and in relation to the use of IT led to rapid development of technical solutions allowing to:

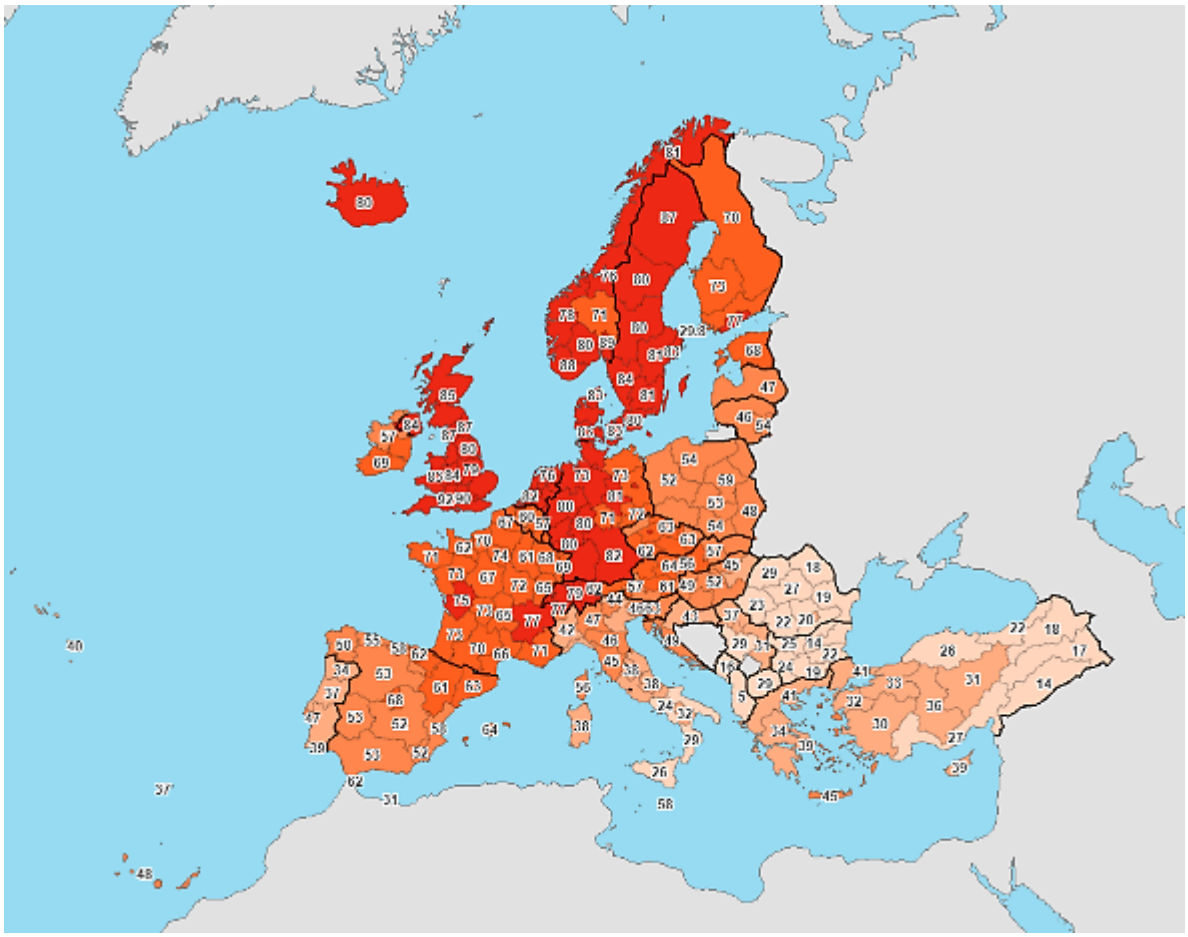
- accomplish tasks using cloud solutions,
- use workflow and management to organize teamwork
- maintain high quality group communication
- ensure cross-thematic cooperation (calculations, estimation, programming, databasing, editing, etc.)

The culture shift caused by COVID-19 pandemic will lead, nowadays and in future, to the emergence of revolutionary cultural and social behaviours, which in 'normal' circumstances would probably evolve in decades. The necessity to isolate and the dependence on telecommuting or hybrid working forced the user of ICT networks, including software providers, to adapt to conditions of the new environment. The most important of these new requirements are: efficiency and efficacy of group communication, the capability to transfer data, information and knowledge capabilities within an organization, and systematization of information, User Experience, and User Interface.

It is important to keep in mind that the development of information technologies and the cyber domain leads to the increase in the scale of threats and dangers appearing in the cyberspace.

In the context of company management and the functioning of information society, it may be concluded that information technologies, and particularly telecommuting and operating in cyberspace, are becoming indicators of innovation, modernity and organisational efficiency. What is more, it is more and more difficult to point to an organization or an area of social life which is not heavily dependent on the use of IT.

The figures below present the demand for the daily use of the Internet and demand for goods and services. Eurostat data show a high level of Internet use in daily life across the whole of Europe.



Bearing in mind the indicators shown above, it seems more and more important to build social awareness of cybersecurity, not only among IT specialists, but also among all Internet users.

Also, military technology and equipment is heavily influenced by the development of IT. Advanced technical solutions are employed in military equipment, e.g. 155mm Crab SPH, BSP FlyEye system, F-35 Lightning multirole combat aircraft. Command posts in command systems are also a special point where information technologies are used, which make them potentially vulnerable to threats. Moreover, besides standard ICT equipment, many systems for aiding information and command processes occurring at various echelons of the Polish Armed Forces. A variety of IT solutions are used in the military at all echelons, starting at the level of a section and finishing at General and Operational Commands.

Cyber Security Training Centre of Excellence (CST CoE) is addressing both societal and military cybersecurity needs. Accomplishing its mission, the centre develops competences of professionals working for the Ministry of National Defence and for the entities of the National Cyber Security System (cf. the Act on the National Cybersecurity System of 5th July, 2018), such as operators of essential services and digital service providers.

In this era of evolving and increasingly widespread information technology – cybersecurity education and knowledge is becoming absolutely essential.

Increasingly significant development of information technologies including: group communication, remote working, cloud solutions, shopping and electronic payment systems will force users of cyberspace to develop competence and knowledge related to vulnerabilities of information systems and technologies, threats and current techniques for gaining unauthorized access. Educating the information society on cybersecurity is becoming a necessary requirement, because as information technologies evolve, more and more areas of society are correlating with these technologies and, simultaneously, are becoming more and more vulnerable.

CST CoE, through specialized and dedicated trainings, such as CyberBEZPIECZNI or Cyber Range training, contributes to enhancing and developing skills in building and maintaining a secure cyberspace, also within the National Cyber Security System. First and foremost, however, it meets the training needs of the personnel of the Polish Armed Forces, both in terms of basic cybersecurity training and in terms of improving the skills of modern weaponry users. This task is fulfilled by means of basic and specialized training courses in the scope of safe operation, configuration and protection of data communication elements of armaments. At the same time, the Centre continuously and systematically develops specialist and expert competences of its staff as an element of the process of long-term planning and educational needs satisfaction in the area of cyber security for the PAF.