Table 1: Summary of R&I needs and priorities

	HYPERCONNECTED WORLD	COMPUTATIONAL SECURITY	INTELLIGENT SYSTEMS	CYBERSECURITY IN LIFE SCIENCES (CYBERBIOSECURITY)
NOTEWORTHY CHALLENGES AND GAPS	1. Generating a broader understanding on how hyperconnectivity may influence humanity and the social and political dimensions.	1. Lack of skills in cryptography; 2. Reduced number of market opportunities; 3. The need for standardisation; 4. Efficient support for developers working in the field; 5. Moving of cryptography research from communication fields to being embedded within hardware.	1. Better understating of socio-economic implications with Artificial Intelligence (AI) applied to cybersecurity; 2. Develop technical and regulatory excellence; 3. The need for foresight and development of institutional capacity to deal with AI.	1. Defining the security implications of life science technologies for cybersecurity research; 2. Skills and training for life science researchers; 3. Generating a broader understanding of the implications of cybersecurity for life sciences research.
RELEVANT FUTURE RESEARCH NEEDS AND PRIORITIES	1. The redefinition of the boundaries of human-computer interaction, and the concomitant security risks that are associated with this; 2. Cybersecurity in the context of new generations of mobile communications and data collection or processing methods (evolution from 5G to 6G).	1. Efficient implementation of symmetric key schemes at higher security levels; 2. Planning and preparation for the transition to the Post Quantum era of cryptographic systems; 3. Secure implementations of cryptographic systems are needed that resist side channel attacks; 4. New assumptions and seemingly-impossible results for future cryptographic components that derive from mathematics, physics or hardware limitations; 5. Standards for new quantum resilient safe algorithms and protocols.	1. Linking vertical and horizontal views on AI research (across research teams but also from design to implementation); 2. Design of approaches for monitoring large-scale and possibly interconnected systems; 3. Exploration of biomimetic cybersecurity algorithms; 4. Inclusion of context awareness in machine learning (ML) in order to boost resiliency.	1. The evolving risks and the threat landscape in biotechnology R&I. 2. Risk management framework in the field of public health microbiology (e.g. modern DNA sequencing); 3. Categories of bio vulnerabilities in the context of cyber; 4. Identification of processes and routines throughout the life science fields that require cyber-interfaces and reliance on automation; 5. Pursuit of various activities and initiatives to establish cyberbiosecurity guides and standards.