Miklós Szócska – Tamás Joó

Health security issues

Miklós Szócska PhD, Director of Health Services Management Training Centre of Semmelweis University
Tamás Joó, Health Economics Analyst at the Health Services Management Training Centre of Semmelweis University

Abstract

This chapter aims to clarify the framework and the different definitions of health security as well as to assign its most prominent challenges. Epidemics and pandemics, activisms on vaccinations, emerging new viruses and bacteria strains, the new challenges originating from lifestyle and altered health behaviour, the role of sovereignty in decision-making will be discussed during the subchapters in more detail. Thanks to the vaccination system of Hungary, classic epidemics do not threaten our country; however, certain opinions appearing in social media on vaccination give rise to concern. The new, emerging resistant bacteria strains are having significant effect on a number of sectors of the national economy, therefore, multisector collaboration is inevitable to reduce the risk. Additionally, the increasing spread of noncommunicable diseases manifest itself in new challenges. When providing answers and solutions to the challenges it is essential to assure sovereignty as well as supporting long term decision making instead of adapting short term decisions. In this chapter healthcare as a source of data will also be described and a short analysis will be carried out concerning the challenges and health security risks in the field of healthcare data collection.

Keywords: health security, pandemics, vaccine, data analysis, biologic, chemical, radiological materials, social media, healthcare, ebola

Introduction

Our personal security concerns are present in our everyday life. We take care of our valuables when travelling on packed vehicles, air passengers got used to airport security measures and citizens collaborate with the authorities in case of natural disasters or terror threat. We rarely think about health security, only usually when we are threatened. The rise of worldwide pandemics, food poisoning, quarantined cruise ships, infected animals to be slaughtered, sudden deadly infections, hospital infections and news about healthcare institutions on the verge of insolvency usually reach the stimulus threshold of the different news networks. Since the centres of worldwide pandemics are far from us, most of us do not even think about the tangible dangers and worldwide background trends threatening the security of our health and of the systems set up to enhance or restore our health. Most of the times we speak about our health and health prevention with our general practitioners or our close relatives and we gain experiences and make judgments concerning healthcare during our personal or family visits to clinics and hospitals. In Hungary, the media informs the public most notably along the health policy programmes and developments and public health campaigns, maybe scandals that fit into the political communication.

As a first step, it is worth clarifying what we mean by health security. International literature lists these issues under the definition of *health security, global health security* (GHSA, 2014). Primarily and in the narrow sense of the expression, challenges of biologic, chemical, radiological materials, worldwide pandemics or pandemic influenza and the tasks of epidemic control are grouped into the subject area of health security. In the European Union and in the world in general, health security as well as health policy and the arrangement of healthcare is considered a national responsibility. It is a common experience that if we address countries that are unable to defend themselves against epidemics with epidemiological and health safety interventions, then these countries consider it as a violation of their sovereignty, and the course of urgent interventions freezes. In the most recent times, however, by way of global connectedness, initiatives for global collaboration and mobilization have enhanced. *World Health Organization (WHO)* is also setting up their emergency medical teams in the framework of global mobilization (WHO, 2014), certain major powers downright initiate setting up groups with special worldwide sphere of authority concerning epidemics which is fiercely opposed by other major powers. The authors themselves who deal with health security are also forced to exceed the narrow definition of health security when they face new challenges or they have to deal with other sectoral or social factors that define health security. We are convinced that the domain of health security should be defined in a sense that is much broader than its textbook definition, therefore we use a more courageous definition and we construe health security issues along broader criteria. From their 1991 strategy (NATO, 1991) on, the NATO our safety and federation ally also uses a broader approach which is also of help for us.

Margin for interpreting health security

In this subheading, we are trying to summarize the most important challenges of health security and the relevant tasks: we give a short definition for health security and list safety policy, health policy, professional and the citizens' tasks with short explanations. In the last century, mankind has achieved impressive results against the main epidemiological challenges and challenges related to biologic, chemical, radiological materials that threaten the basic conditions of the biological existence of the human race and eradicated pathogenic agents that used to be able to depopulate even a continent. However, we need to be aware of the fact that nowadays the leading causes of death are not communicable diseases and worldwide pandemics but chronic, non-communicable diseases, i.e. diseases resulting from our lifestyles. Therefore, we have to classify several other factors into the subject area of health security which affect the health of the nation, the vulnerability and sustainability of the health prevention and health recovery system or the sovereign decision-making related to them and its influence.

Information technology improvements not only established new opportunities, but also brought new health security challenges to society. Hungary is not an exception to this either. In Hungary, health accounting systems have been functioning since 1993 which result in the generation of a large amount of electronic data. The security of and the use of these data for safe treatment, research and decision-making purposes is also a strategic fundamental question regarding health security.

Another study in this volume addresses the issues related to the access to clean water and the threat to the clean water supply. The traditional health security considerations regarding chemical and radiological materials are well-known and obvious since Chernobyl or the Hungarian red sludge catastrophe. What we breathe in, what we eat or drink, what is absorbed through our skin, the noisy environment, the materials of the built environment, the new chemical materials, the appearance of contraceptive hormones in our waters—there are detailed studies regarding all of these factors that affect health and even fertility and population growth. Complex researches demonstrate the relationship between the worse morbidity statistics of the people living near airport runways or the incidence of lung cancer in people living in the smog in a developing economy, however, in general at present the considerations of short-term economic interests are globally stronger than that of long-term sustainability. SDG *(Sustainable Development Goals)* is a significant experiment in order to emphasize the issues of sustainability, including the issues of the sustainability of health (UN, 2015). Nowadays, these principles apply without an implementation strategy and institutional fundraising, on the level of a globally adopted declaration.

The response potential of Hungary to the challenges of biologic, chemical, radiological materials concerning epidemics is exemplary even in an international comparisons due to the hygienic civilization, the advancement of the system of vaccination thanks to Semmelweis' heritage and the lessons learnt from the efforts made in order to overcome tuberculosis. From the epidemiological point of view Hungary is safe, we have a suitable biologic, chemical, radiological institutional system in place to take care of health security. In the past decades, this institutional system has been reorganized several times in order to enhance its efficiency for which the reason was the inertia of the overgrown bureaucratic system. The experiences of the series of reorganizations are still to be processed in several aspects. On the one hand, it is vital to maintain the operational character of our health care system during the reorganizations. On the other hand, it is still not sure whether our healthcare authorities working along bureaucratic solutions are able to demonstrate sufficient flexibility against the new challenges. Thirdly, the extent to which short-term industrial policy interests prevailed against long-term health interests during the reorganizations is still a question.

Challenges of health security

Worldwide pandemics in the form of emerging diseases pose a previously unknown threat. Avian influenza, ebola and zika pandemics demonstrate well the types of challenges mankind have to face as a consequence of global warming and environmental changes (Patel, 2015). Unknown pathogenic agents become activated and the so-called vector organisms (e.g. certain species of mosquitoes) which "transport" them gain living space where they have not been expected to appear so far. Due to globalization, Hungary is exposed to the danger of worldwide pandemics, even if these are expected to outbreak in distant continents. We have safety laboratory and vaccine production capacity with regional competences, our experts participate in the global control, however, they are working under tight financial conditions. The experiences of flood control, the solidarity in these cases and the existence of a united disaster management organization equips Hungary with the ability to take appropriate actions in case of a crisis.

The real question concerning worldwide pandemics occurs on the global level. Will we be able to predict the emerging worldwide pandemics, recognize them in time and to mobilize enough resources for technological development necessary for their control? Are we able to organize the support of the developing world in an epidemic emergency and to communicate correctly via global mobilization and cultural sensitivity? How fast will we be able to develop vaccinations and medicines against the new pathogenic agents (Wolicki et al., 2016)? After the frightening experiences gained regarding the previous avian influenza and later ebola pandemics (Heymann et al., 2015) major progress has been achieved in the communication during the control of the zika virus, however, even this could not offset the press panic following the correct professional communication, which seriously affected for example the organization of the Olympic games in Rio. This phenomenon demonstrates well that not only pandemics but also the distorted perception of the dangers related to them and the unnecessarily heightened sense of danger and scaremongering may also have serious consequences. The epidemics risk, the management of pandemics depend on civilizational development and health literacy.

Vaccination and activism

Trust in the Hungarian vaccination system plummeted during the political scandal related to the non-transparent vaccine production contracts of avian influenza epidemics. After 2010, the vaccination system has been successfully stabilized and in 2013 extended along the consultations with professional medical organizations and patients' associations. In the first year 80% of the parents requested HPV vaccination for their children—based on this and the high vaccination rates on the global level, it can be stated that the Hungarian vaccination system performs exemplary. Industry-trade lobbying and anti-vaccination activism are the two factors that are of moderate threat to the vaccination system. The trust in the vaccination system can be easily shaken by an uncertainty concerning procurement. The tactical elements of the industrial competition for the markets (the competition of the market operators concerning the procedures) may easily damage the procurement, delivery and, as a consequence of the former, the vaccination deadlines. Based on the analysis of the Hungarian-language Facebook groups, anti-vaccination activism can be considered limited, they intervened unsuccessfully during the introduction of HPV vaccines. However, in recent years the international anti-vaccination lobby has expanded in a dangerous and spectacular, Hollywood-like manner. There are religious communities worldwide which are against vaccination or other medical interventions. Many of these operate serious epidemic information systems in order to protect their adherents (e.g. protestant fundamentalist groups in The Netherlands). Due to its vaccination rate and hygienic development, Hungary is not threatened by traditional pandemics, not even as a consequence of migration. However, due to wars and regional conflicts millions of people are becoming inaccessible for the vaccination systems. Therefore, maintaining the vaccination rate, the continuous development of the vaccination system the transparency of the procurement system and following the activism are fundamental interests of health security and these should be treated as a subject area of constitutional protection.

Resistant bacteria

From an epidemiological point of view, the resistance of pathogenic agents against antibiotics is the next health security challenge. Resistance has been developed due to human and animal medicine practice. Irresponsible medical practice, the patients' poor medication adherence, failure to cooperate (*compliance, adherence*) and antibiotics administered irresponsibly and in great quantities in order to increase farming yields in agriculture as well as the lack of control all contributed to the development of pathogenic agents that are resistant to antibiotics. Two more factors hastened the premature exhaustion of the most advanced antibiotics. On the one hand, the medical profession, the researchers and the pharmaceutical manufacturers have been following with euphoria the spectacular results in the combat against infectious diseases and have already begun to talk about the end of the era of infectious diseases. The desire and inclination to research diminished, the industrial innovation investments available for antibiotics development flooded to other, more profitable sectors, production profitability has declined sharply. On the other hand, marketing related to the introduction of the new generation of antibiotics also had an adverse effect. Doctors want their patients to heal quickly and surely so they tend to choose the medicine that has the best possible results, while patients try to get the medicine that shows its effects sooner. As a result, mankind has used and exhausted the newest generations of defensive tools against bacteria sooner than expected therefore it might be left without effective protection. It is vital for mankind and for the governments and authorities to find new forms of protection against one of the most important challenges regarding health security by way of professional mobilization, regulation, control, investments and incentive business models and coordinate the aspects of human and animal medicine as a coherent whole. Sovereign decision-making that controls related short-term business interests is a vital issue that affect the fate of mankind.

Health security in treatment

In the context of healthcare, by health security we mean the reduction and the prevention of the occurrence of unintended harm related to healthcare and guarantee of patient safety. The notion of adverse event refers to a negative event that is the consequence of healthcare and is not linked to the disease itself, as, for example, a damage resulting from a wrongly administered medication or a hospital infection developed after a surgery. In the background of these, the weaknesses of healthcare processes are usually identified. The incidence of adverse events therefore closely connected with the organization of healthcare.

Two forms of adverse events may occur: on the one hand, we can speak about preventable events (e.g. confusing medications in similar packaging) which can be avoided through appropriate measures and process controls, on the other hand, not preventable events (e.g. the development of unknown allergic reaction to a medication that have not been administered previously).

Errors do not always lead to an adverse event. If the error is detected and corrected in time it is the so-called *nearmiss* (e.g. when the patient's right eye is prepared for the surgery and during the checking of the administration—still before the surgery—someone notices that it is the left eye that needs surgery). The detailed analysis and research of near misses and actually occurred adverse events is of utmost importance for the prevention of events evolving later and for similar reasons. Finding systematic errors and learning from them are supported by the anonymous patient safety report and learning systems. In Hungary, the "unexpected events" (NEVES) report system and the recommendation for the management of single, serious adverse events called "procedure for the management of unexpected events" (NEKED) was developed according to the WHO recommendations published in 2005 (Lám et al., 2016).

Besides the analysis of the report results, detection and management of healthcare risks, of process control, the application of protocols and directives, the arrangement of responsibility relations and the development and sustainability of organizational culture supporting patient safety all play an important role in the prevention of adverse events. Therefore, for example, a special healthcare risk factor is *burnout*—among other things, this is an aspect that makes the earlier high rate of doctor and nurse migration a health risk in Hungary.

Health security aspects of health

In the field of health security, citizens have an active role as our habits and lifestyles can influence the fulfilment of systemic goals. The health security measures' aspects related to public health diseases and death and budgetary matters are the fundamental questions of the sustainability of a nation, a country. How long do we live? Moreover, how long do we live in health and illness? Compared to our rivals and allies how will the health and mortality of the population evolve? What resources are available to us?

In recent years, Hungary has become the focus of international attention in this area as during the peak of the global economic crisis it has been able to quickly take such pioneer, sovereign and significant health policy measures, such as the total ban on smoking in closed public spaces, the introduction of public health product tax (NETA), enforcing the trans-fat content of foods below a safe limit value, introducing everyday exercise in schools and strengthening and expanding the vaccination system. In Hungary it has also taken the regulation in favour of smoke-free environments a long time to be passed which otherwise was supported by the majority (even smokers). Smoking has proven to be harmful to health, prohibiting it saves lives and health. The life years lost, healthcare costs, the production losses because of sick leaves as a burden on national economies have also been proven to outweigh the related budget revenues. Parties having adverse interests – groups thinking that the ends always justify the means – could successfully hinder the adoption of more stringent regulations in many countries. Their main arguments – typically the loss of jobs, the flourishing of the black market and the economic loss due to tax revenue losses – lead many economic and political decision-makers to withdraw. Withdrawal happens in spite of the fact that smoking threatens the national economy and in particular the sustainability of social and healthcare systems through diseases, sick leave or even through the exorbitant costs of oncological treatments and the consequential economic burden of death.

Public health product tax (NETA) is a leading example at international conferences on public health. It is known as an innovative fundraising tool which can simultaneously achieve with 40% of the manufacturers the reduction pf the quantity of salt and sugar added, the 25-35% reduction of consumption and the creation of the basis for wage increase for doctors and nurses (WHO, 2015). Levying the NETA had multiple objectives: on the one hand, similar actions motivate the industry to make profit with more healthy products. A global food company announced recently that by changing the structure of sugar crystals it was able to significantly reduce the sugar content of its products allowing a nearly identical perception of sweetness. This result is a good example of the fact that the industry is trying to adapt to the ever-increasing demands of movements related to food limit values. On the other hand, however, opposite direction lobbying becomes active, stronger and refined. Luxury goods that are sweet, salty, can be smoked or drunk result in burden of disease via addiction related to them. The vital interest of the industries that benefit from this is maintaining and achieving the most permissive regulation. The aspect of regulation related to health protection will have its breakthrough results only decades later. Therefore it is a key question whether we make decisions regarding healthy eating, smoking and alcohol consumption in a sovereign manner or individual or probably industry interests prevail in the decision-making.

The regulation related to health protection will have its results only decades later. Based on the logic of the national budget, a decline in 10-15 years' time regarding sick leave or premature death is difficult to interpret now regarding the budget balance. At the same time, the results that can be achieved via regulation are well illustrated, for example, by the 2-3 decades shift of the peak of US smoking and lung cancer mortality rate as well as that of the downward curve (see Figure 1) (The Tobacco Atlas, Fifth Edition, 2015).

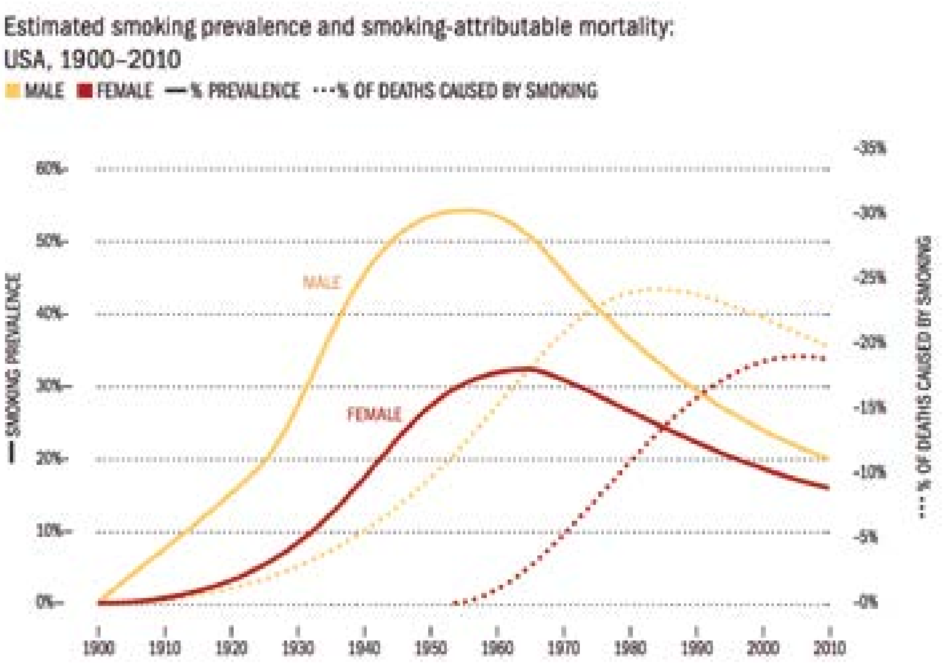

Figure 1

Estimated smoking prevalence and smoking-attributable mortality of men, United States

Source: The Tobacco Atlas, Fifth Edition, 2015

Therefore, in our country which tops the lists of cancers and cardiovascular diseases and has a low reproductive rate, the long-term maintenance of health protection regulations is of vital interest. These regulations are to be construed as a long-term sustainability investment and their loosening constitutes a health security risk. This is why it is justified to follow the influencing activities regarding these issues on constitutional protection level.

Sovereignty in decision-making

The issues concerning the sustainability of the supply system and the sovereignty of the decisions related to the supply system are also grouped into the subject area of health security. Maintaining a sovereign decision-making space is a fundamental national interest. The influence of this due to opposite economic or other interests arises as a fundamental question of sustainability and health security. Are we able to produce the most health benefits from our scarce resources? We can bring together enough resources to maintain the risk pools? What medicines do we spend money on and how much do we pay for them? Do our procurement systems achieve the most effective results? What kind of instruments and what size of instrumentation do we work with and how effectively do we use it? How many do we spend on their procurement and maintenance? Are we able to manufacture or produce the strategic stocks or do we have to purchase them elsewhere?

Over the last decades, the issue of the supply system and its certain components and the privatization of our health financing system and the development of capacities have been repeatedly on the agenda. Beside the fact that within the framework of our constitutional system we are certainly free to decide on the supply systems, it is reasonable that efficiency issues are key factors in decision-making. Experiences with hospital property or with outsourcing and privatization of certain critical service or profitable hospital substructures (diagnostics, pharmaceuticals) is negative. Privatized institutions or institutions with privatized management were not sustainable, they got deeper into debt compared to institutions of similar size. The social consequences of privatization attempts were always end up to be guaranteed by the state or the local government. In all the cases, an important strand of privatization attempts was moving the suppliers within in the sphere of interest of the owners into hospitals (from the buffet through the supply of medicinal products even to hiring hospital workers from services companies). Thus, it can be stated that profits associated with operation were privatized whereas the negative consequences related to operation and sustainability in every cases appeared on the level of the state or the taxpayers. The privatization of the social security system at the dawn of the global economic crisis have luckily failed. As a thought experiment, however, it is still worth following through what would have happened to the assets of our privatized social security funds or with the resources of healthcare during a world crisis. These are resources worth hundreds and thousands of billions of Hungarian forints therefore the influence of the related decisions is a natural supplier and investors' interest. The fundamental question is that how sovereign efficiency considerations are during decision-making and to what extent intentions to influence and effects are obvious to the decisionmakers. What is at stake is how much health benefit we are able to produce or restore with limited resources and whether social justice concerning the availability of healthcare is damaged; whether the imbalance of this (e.g. the burdens of the waiting list of people with no influence) jeopardizes social peace. These considerations are applicable to the questions concerning both the fundraising and -managing social security system and the management of the supply system and its components.

Different activisms regarding health security

In health security issues related to the health care system, special attention is paid to the political and interest protection activism. A good example was the healthcare strike in 2012 in Slovakia in which professional and labour organizations began to fight for wage increases. Night shift workers abandoned their workplace and those who worked on the day shift did not come to work. According to reports, patients on pulmonary ventilators at intensive care units were left unattended and the management helplessly tried to recruit temporary workers from the neighbouring countries. Their such attempts were hampered by the fact that the persons on strike had coordinated their action with the doctors' association of the neighbouring countries so only a limited number of volunteers and army surgeons arrived. Special attention should be paid to the form of the organization of the strike. Not all the doctors have been invited to strike, only the ones who disposed over workflow that is critical from the point of view of cure, i.e. who work in the fields of intensive care, surgery, traumatology and gynaecology. Not all the representatives of the professions playing central roles participated, however, the exit of this critical mass from the system did result in the disruption of it. Later the collection of the signatures of Hungarian residents also aimed at central actors and threatened with the possibility of the disruption of the healthcare system. The different phenomena naturally associated with civil democracy highlighted the vulnerability of healthcare systems: the system can be quickly paralysed by an attack at the allocation points of scarce resources.

All these draw attention to the procedures, the rules of healthcare safety and to the need to plan the capacity and logistics of the preparedness for critical situations. These principles are also true to the reconsideration of the vulnerability of the critical central elements of healthcare infrastructure. To avoid misunderstanding, it is important to underline that this is not to express reservations concerning political activism; however, we must see that in certain cases activisms aim at proving the malfunctioning of the healthcare systems, even at the price of causing the system to fail.

Examples of different social activisms are those organized around religious criteria which, in radical cases, are not content merely spreading their doctrines but also attempt to enforce them onto others even by influencing state authority. These may include doctrines pertaining to the prohibition of tissue reception or transplantation which may result in damaging or destroying valuable life-saving stocks. Such an activism may result in hampering professions (e.g. psychiatry) prohibited by religion and their institutions. Religious activism is usually paired with medicine-related trade, fundraising and profit-making quackery that is harmful to health. Animal welfare activism, in particular if it affects the animal houses of priority laboratories (or laboratories related to epidemiologic safety) also poses a health security risk.

Health security, decision support, data analysis

Information technology improvements have not only established new opportunities, but have also brought new health security challenges. Hungary is no exception to this either. In Hungary, health accounting systems have been functioning since 1993 which result in the generation of a large amount of electronic data. The security and the use of these data for safe treatment, research and decision-making purposes is also a strategic fundamental issue regarding health security.

One of its aspects is the availability and safety of patient data. Data, especially data available in time, saves lives. We may forward patient data from the ambulance, the ambulance doctor may search for the place of regular care of the unconscious patient or supply electronic healthcare services to chronic or acute patients. Moreover, if our doctor has access to our diagnostic data, we are able to save public funds by the abandonment of any unnecessarily duplicated procedures. However, such data are confidential, therefore their safety is a prime factor which raises serious technical and work arrangement questions through governing the eligibility and technological security. The influence of the Iranian nuclear program is a good example for the damage a digital attack may cause in the physical infrastructure. This logic may affect even medical devices.

There is a worldwide combat for the control over data. Social media service providers and smartphone ecosystems began to introduce applications that collect data regarding health and lifestyle. On the one hand, the availability of applications regarding lifestyle, which may even have impact on public health, is to be welcomed. On the other hand, big data may help the researchers understand diseases, discover new treatments or develop therapeutic artificial intelligence. It is a question of health security as to who controls the data. Do data serve private or public purposes or maybe quackery marketing or other trade activities that violate the ethical boundaries of healthcare? Therapeutic data may support the organizers of healthcare and even suppliers to make immediate business decisions. Which medicines are prescribed by the doctors, what kind of illegal incentive should the manufacturer pay? What kind of medicine heals the patient, what should be a part of the healthcare protocol? Therefore the use of data saves lives and public funds and is also suitable for marketing and for facilitating decision-making related to system efficiency. Obtaining and controlling of the data is crucial therefore it needs to be managed as a health security strategy issue. Social media service providers and multinational companies which supply hospital information systems acquired competitive edge in a hidden way, however, data protection fetishism characteristic of the 20th century healthcare does not address the hazards involved in this. Nowadays 21st century data strategy responses are needed to address the issues of control over data, public access to data should be provided and vulnerability of the individuals and communities against monopolistic data controllers should to be prevented.

The genetic data used for the highly developed technological diagnostics and treatment of cancers is of particular importance. One of the most promising therapeutic option is the precision treatment targeted based on the genetics of cancers. This means the medication is administered by targeting based on the genetic material of given cancer cells. This technology raises the theoretical possibility of administering genetically targeted toxins into groups of people with given genetics. This opens up a possibility of a real genocide. Mining genetical information and building data bases are vital for the development treatments for diseases that are incurable today so the management of these problems should be addressed. However, we have to be prepared for the management of the hazards involved in this so conducting related philosophical and ethical debates is imperative.

Summary

In this study, after linking the subject areas of healthcare and safety, we discussed the interpretative framework of health security in particular regarding global tendencies in diseases and the Hungarian institutional system. We discussed in details the main challenges of health security we are currently facing such as activism regarding vaccination, the resistant bacteria, patient safety, the role of health, sovereignty, and the importance of data analysis.

General experience regarding health security is that the breakout of worldwide pandemics causes alarm, opens up the channels of donation and later, as the danger passes, attention deteriorates, donations cease and the resources for the investments necessary for systemic control are not available. At present, WHO's emergency fund is filled up to 25–33%. Moreover the budget for the defence lines of epidemiology and 20% of the entire staff of WHO are cross-financed from donations given for the prevention of polio. Donations for polio that can be overcome in 1-2 years cease in 1–2 years, and WHO does not even have an organizational unit engaged in fundraising. Nowadays, global health security control depends on occasional donations. One particular individual along with other donors engaged by him play a prominent part in the life of the institutions of epidemiological control. Bill Gates, the billionaire-president of Microsoft has raised a donation of critical amount. In the lives of the institutions, the exposure to, and the dependence upon, the critical resources received from a single source is a risk factor in itself. There are not even discussions concerning the mechanisms of institutional fundraising. During an epidemic that is similar to ebola, the expert arriving from the northern hemisphere to the countries of the southern hemisphere was asked questions such as the following: What epidemic did you come to help with? Ebola? How many people die of it? 11 thousand? And of malaria? And how much do you care about the man dying of it? Or are you just worried about that the ebola will reach you by plane and will spread quickly? The questioner was not far from the truth. In our combat for the dominance of life on Earth collaboration for epidemic control and strategic thinking is carried out by isolated, financially vulnerable institutions and mission-oriented people and professional workshops. The answers currently available are unsatisfactory.

References

American Cancer Society (2015): *The Tobacco Atlas.* Source: http://3pk43x313ggr4cy0lh3tctjh.wpengine.netdna-cdn.com/wp-content/uploads/2015/03/TA5_2015_WEB.pdf (21.01.2017)

GHSA (2014): *What is GHSA?* Source: www.ghsagenda.org/ (21.01.2017)

Heymann, David L. – Chen, Lieping et al. (2015): Global health security: the wider lessons from the west African Ebola virus disease epidemic. *Lancet,* Vol. 385, No. 9980. 1884–1901.

Lám, Judit – Sümegi, Viktória – Surján, Cecília – Kullmann, Lajos – Belicza, Éva (2016): A jelentési és tanulórendszerek szerepe a betegbiztonság javításában (The role of the reporting and educational system in improving patient safety). *Orvosi Hetilap,* Vol. 157, No. 26. 1035–1042.

NATO (1991): *The Alliance's New Strategic Concept.* Source: www.nato.int/cps/en/natohq/official_texts_23847.htm (21.01.2017)

Patel, Mahomed S. – Phillips, Christine B. (2015): Health security and political and economic determinants of Ebola. *Lancet,* Vol. 386, No. 9995. 737–738.

UN (2015): *Sustainable Development Goals.* Source: https://sustainabledevelopment.un.org/?menu=1300 (21.01.2017)

Wolicki, Sara Beth – Nuzzo, Jennifer B. et al. (2016): Public Health Surveillance: At the Core of the Global Health Security Agenda. *Health Security,* Vol. 14, No. 3. 185–188.

WHO (2014): *Outbreaks and Health Emergencies.* Source: www.who.int/about/structure/organigram/hse/en/ (21.01.2017)

WHO (2015): *Public Health Product Tax in Hungary: An example of successful intersectoral action using a fiscal tool to promote healthier food choices and raise revenues for public health. Source:* www.euro.who.int/__data/assets/pdf_file/0004/287095/Good-practice-brief-public-health-product-tax-in-hungary.pdf?ua=1 (21.01.2017)

József Bokor

An introduction to the examination of security issues in cyber-physical systems

József Bokor, full member of the Hungarian Academy of Sciences, Vice President of the Hungarian Academy of Sciences, Scientific Director of the Institute for Computer Science and Control of the Hungarian Academy of Sciences

Introductory thoughts concerning the subject of cybersecurity and cyber-physical systems

The virtual space – the so-called "cyberspace" –, made up of interconnected computer networks, has undergone an unprecedented expansion during the past decade. To an ever increasing extent, state and government bodies, companies and individuals require the ability to integrate the benefits of their online presence into their daily activities. The *World Wide Web (WWW)* has been the predominant technology for the past several decades to share electronic content around the world and retrieve it according to specific criteria. The enabler of leveraging the technology and making it accessible globally to everyone was made possible by the improvement of quality and reliability of the underlying technologies (e.g. network building and server technologies, virtual machines).

As the spatial expansion of cyberspace continues and the density of its supporting resource systems increases in the technologically advanced regions of the world, maintaining the reliability of services and the security of contents turned out to be the greatest challenge ever for the traditionally open and innovative digital technology, offering open access for everyone. At the same time, the advanced engineering systems of the future that emerged in the recent years are a product of a symbiotic approach to process control and informatics, creating a qualitatively new situation in the area of technologies previously described only as safety critical. Traditionally, safety critical systems are described as *standalone* engineering systems and applications the operation of which come with inherent risks of life threatening accidents and/or serious damages to the economy, the environment or even the society if they malfunction. Such systems include vehicle and aircraft control, applications in the chemical industry and in nuclear power plants, but also banking applications.

Cyber-physical systems are safety critical systems operating in the cyberspace: their physical implementation involves (embedded) computers, with a complicated network of connections between them, that collect data over various networks, monitor and control complex physical processes, manage sensors and actuators. The prevalent applications of cyber-physical systems have a significant impact on our daily lives thanks to the exceptional degree of their adoption by the society: they can have a profound influence on our quality of life and on the efficiency of the contribution of industry, healthcare, education, and any other systems that are part of the private sector, and/or of an economic player to the national economy; they determine the state of the environment and the general conditions of community work. However, if they malfunction or if they deliver corrupted or maliciously altered content, these system may also be capable of causing accidents claiming human lives, service disruptions in entire regions, damages to properties, and environmental disasters, and as such they should be regarded as systems and technologies that have national security related implications, belonging to the critical infrastructure, and should be prioritized both in the design stage and in operation. For this reason, protecting the critical infrastructure has become a primary objective of modern societies. Technological progress comes with a number of benefits and opportunities, but it also carries new security risks and social challenges. Implementation and sustainable operation of cyber-physical systems introduce new challenges in terms of protecting the security of the cyberspace.

The *number of risk sources* or, in other words, the *threat* increases in proportion to, or – according to certain opinions – at a rate significantly exceeding the growth of the size of networks, which can be explained by the fact that the root causes of emergencies are mostly coded into the technological systems as structural sources of faults and failures. Operation in an incorrectly selected architecture carries structural risks. The *risk degree* has a distribution pattern that shows geographically varying densities, and is related to how advanced the local technology is. The fluctuations in the density distribution of services are characterized by the inherent proclivity of *large-scale* networks to form hubs as a result of their *(scale-free)* network organization and growth characteristics. Over the conventionally fault-tolerant, highly distributed connection systems of the Internet a highly vulnerable service delivery system built on centralized distribution/service hubs is formed, which increases the interdependence of system elements, and requires a system-level approach to the handling of vulnerabilities.

Reducing the openness of the system cannot be used to increase the security of cyber-physical systems as the operation of these systems rely on uninterrupted connectivity, which is characterized by a pool of redundant and highly distributed resources and cooperative task execution. One of the most important questions is how risks can be reduced by implementing security measures to block attempts at disabling or impairing technologies without restricting openness and accessibility that are regarded as essential in the context of those technologies and the society.

Preventive and countermeasures can be divided into two major groups. There are so-called *design-stage* considerations and there are *operational-stage* methods that can be applied to the operation of the rolled-out systems. For example, it is a design-stage consideration that the least vulnerable and self-repairing architectures should be created. When the architecture of cyber-physical systems with significant operational risks is designed, the security analysis, that is part of the design process, will involve maximizing the permissible statistical frequency (risk) of malfunction by a probability value proportional to the amount of damage caused, requiring that the probability of an unwanted event should never exceed this threshold.

In order to meet security requirements, the most critical cases may necessitate the use of fault tolerant solutions. Fault tolerance is the property of a system that allows it to restore its original functionality by recognizing anomalous changes in its operation (resulting from malicious interventions, tampering with data, component failures or any other external effects that have an impact of any kind on the integrity of the system). Fault tolerance, as a design property of the system, is an autonomous operational feature based on the detection of faults and failures and any other unwanted changes, aiming at restoring normal operation immediately.

Up until recently security issues of cyber-physical systems providing critical functionality were addressed typically in the area of network infrastructure protection and fault-tolerant control design. *Accuracy, integrity*, and *reliability* of data collected and processed by the system and their impact on security were given little though in the evaluation of risk factors. The status of sensors and actuators and their interaction with the environment containing the system were not a key part of investigations. This practice led to security solutions that assumed a closed cyberspace where the origin of faults and attacks was likely to be found inside the cyberspace (or, as a matter of fact, in the connection between computers). This approach is well characterized by the fact that, for example, while cryptographically encoded and authenticated *(digitally signed)* data traffic between communication end-points offers a solution for securing communication between two parties in a way that is literally unbreakable within a reasonable period of time and provides efficient defence against unauthorized injection of new data content between the two end-points, it is powerless against the malicious modification of transmitter-side sensor data (or the immediate physical environment of the sensor itself).

Thus, cyberspace should be regarded as an integrated whole containing sensors, actuators, information and network systems; a space with problems that cannot be resolved from the inside without taking into account processes in the environment encapsulating it. This way of looking at the problem may facilitate the handling of security risks in systems by correctly determining their vulnerability directions and treating their security risks as part of their environments, following a *systems theoretic* approach.

As a result, plausibility problems *(trusting)* that were brought up earlier in regard to the malicious tampering of measurement data and the reliability of sensors, should also be addressed as part of a new approach. For example, how can someone be sure that data entering the system provide an authentic representation of reality? Conventional error detection mechanisms of sensor systems which are based on testing the statistical independence of measurement data, are suitable for pinpointing physically damaged sensors or sensors that failed for any other reasons, and isolating data supplied by them. However, these methods cannot be applied to stop sophisticated attacks against the sensor space itself. In order to achieve this goal, new systems that are capable of verifying the plausibility of data must be used.

Through the application of the advanced methods of data science and machine learning, patterns, fingerprints, and regularities indicating normal operation can be extracted from the data entering the system, and then they can be used to detect anomalies. These topics are discussed in the first part of the study in which the author, András Benczúr, applies one of the most advanced methods of data science, the so-called *big data,* to the problem of input plausibility. In doing so, he elaborates the possibilities of the so-called data-driven methodologies (methods using computer-based analysis and modelling of data) in the detection of security risks. Big Data based, typically real-time analytic processes, however, can only be implemented efficiently on an elastic IT infrastructure that offers versatility of access and support for custom configurations. The distributed method of data access, data sharing between the active elements of the system performing the analysis, and cooperative processing lay down the foundations of employing new plausibility checking methods based on the diversity of sources, and as a result, creating robust fault-tolerant systems. Design methods of this infrastructure *(IT cloud)* and the issues of implementing the Bid Data concept are addressed by Róbert Lovas in the second part of this chapter.

In cyber-physical systems, resolving input plausibility issues is a topic subject to real-time constraints. In such cases, control tasks should be taken over by efficiently distributed management and filtering strategies that are suitable for the architecture of the system. Environment perception methods for autonomous vehicles and vehicles systems, such as camera vision based methods, LIDAR (laser) based environment perception technologies, and complex shape, movement and human detection applications ensuring the accuracy of positioning and monitoring community spaces exposed to risks, represent serious scientific challenges in terms of compliance with security requirements. Such problems, including the capabilities and the applications of leading environment perception methods and a presentation of the typical signals and signal processing devices are discussed by Szirányi and Havasi in the third part of this chapter.

The automated transport systems of the future will form an emerging new class of critical infrastructures that, due to the overarching character of the transport sector within the national economy, play a fundamental role in ensuring the security of systems and processes affecting the entire society. Special applications of automated transport systems can be implemented in the domain of driverless ground and aerial vehicles. An overview of the research and development directions of controlling small flying objects that are usually not subject to a permit to fly (drones or UAVs) and the security aspects of integrating these vehicles into the air traffic control system is provided in the closing part of our chapter, by the authors József Bokor and Bálint Vanek.