Jarosław Piątek[1]

TECHNOLOGY "DEMOCRATIZATION". PEACETECH – NEW QUALITY OF SECURITY MANAGEMENT

Keywords: security, new technologies, security management, information and communication technologies, monitoring, observation

ABSTRACT: Contemporary time, interpreted by the prism of security, is no longer dominated by easy to describe inter-state conflicts or regional threats. Experts every now and then define new types of threats such as cybercrime, cyberterrorism or cyberwar. The intense and multi-level uncertainty affects the understanding of the present and the predicted future, and thus the search for security by all of us. The answer depends in part on whether we are able to understand contemporary security environment. These issues are, to my mind, independent of the place in which we are. Using tools for diagnosing and monitoring security remains an open question. At the moment we are searching for a solution to this problem by means of modern technologies. The paper stresses the importance and application of e.g. Internet technology and global telecommunication. Interpersonal relations are being replaced with technological solutions. Nowadays, a phone or a computer connected to the web is sufficient to make contact with another person or check what information official sources are bringing us today. Actions for security as a result of incorrect reception of a message may be associated with erroneous perception of the content and propaganda. As a result, the recipient is consciously manipulated. New technologies take the form of nonconventional, organized activities for security. Any number of people can cooperate through the web for security management without actual superior authority. Members of such

[1] Jarosław J. Piątek, University of Szczecin, Faculty of Humanities, Institute of Political Science and European Studies, jarekpiatek@wp.pl. ORCID ID: 0000-0003-4754-3371

groups, established ad hoc, may use their knowledge to express objections or dissatisfaction. The paper also presents another aspect of using technology. According to the author, there are situations in which technologies acting for reinforcing security often cause objection, motivated by restricting civil freedoms and by the threat of an attack on a free and open society.

INTRODUCTION

A new wave of technologies drives rapid global changes. "Waves" of technological changes, driven by inventions – from steam energy, to electrical energy, to a car – propel economic development and social transformation in the most recent history (Sachs, 2015, p. 82). A lot of people talk about "technological revolutions": the first industrial revolution, which mechanized production, the second, which brought mass production, and the third – automated production. It has been argued that we are now in the phase of the fourth technological revolution in which the fusion of various technologies obscures the boundaries between the physical, cyber and biological spheres (Yáñez, 2017; Latiff, 2018, pp. 43–44). Compared to previous industrial revolutions, the latter proceeds at an exponential, not a linear, pace. What is more, it distorts almost all industry branches in every country, and the breadth and depth of these changes herald a transformation of entire systems of production, management and exercising supervision. It seems that the expansion of new technologies, from the Internet to technologies related to synthetic biology, cannot be stopped. Technological changes have created new possibilities of multilateral cooperation in areas that have been undervalued and marginalized so far, since they create new conditions in managing relations between the state and the society, as well as between countries. New technologies and platforms to an increasing degree already today allow citizens to be involved in governance, to express their opinions, to coordinate efforts for the quality of government and even to circumvent the supervision of public authorities (*Anti-Counterfeiting Trade Agreement* – ACTA). At the same time, governments are gaining new technological opportunities in order to increase control over the society, based on ubiquitous surveillance systems and the ability to control digital infrastructure. Generally speaking, governments will more often need to change their current approach to public involvement and to shaping politics because their main role, that is conducting policies, is getting reduced due to new sources of competition as well as redistribution and decentralization of power which is facilitated by new technologies.

The fourth technological revolution will have a deep impact on the nature of the security of the state as well as, in a broader dimension – of international security, affecting both the likelihood and the nature of potential conflict. The history of wars and international security is the history of technological innovations and it is no different today. What is more, contemporary conflicts involving countries have an increasingly "hybrid" nature, combining traditional combat techniques with elements previously associated with non-state entities. The differentiation between war and peace, the fighting and the repressed, and even violence and non-violence (e.g. in cyberspace, involving cyberwar) is becoming more and more difficult. Because this process is already underway, and new technologies, such as autonomous weapons or autonomous robots and systems, are becoming easier to use, individual entities or small groups more and more frequently have military power that can compete with what countries have. This gap will lead to the emergence of new threats and will bring new concerns. At the same time, technological progress (which is abundant) will create a potential to limit the scale or impact of violence, for instance through developing new ways of protection or greater management precision. Therefore, possibilities to use modern technologies for shaping security are being opened. I do not mean those related to the process of deterrence since it had been going on for a long while now. It concerns new technologies which expand the area of security management and also reduce risks and the resulting crises; technologies, which focus on opportunities and challenges for security. The private sector and the entities of the civil society in particular often play the leading role in the development and the pioneer, innovative use of these technologies, and also in managing their application.

MYTH OR REALITY? PEACETECH – "DEMOCRATIZATION" OF TECHNOLOGY

The development of mass communication networks offers mighty propaganda and recruitment tools. Victories over infidels are announced through social networks, training videos etc. are published there. In order to achieve these targets, influential internet users or hired specialists may be used and special software is developed too. The speed of information transfer is key. Internet is used to disseminate propaganda and for communication with the media while the recipients are kept informed about events. Independent media's favours are sought in particular, which often makes it possible for the message to reach addressees outside of the media and political mainstream (Dyczewski, 2008, pp. 115–116). Thanks to the strong message certain behaviours and social roles are created. Hoffman believes that thanks to the use of information technology Hezbollah in 2006 convinced the international community about the validity of its battle (Hoffman, 2007, p. 39). Mobilization of a recipient occurs, which is used to create desired attitudes towards the causes of conflict and its course.

When analyzing the modern wave of the technological revolution, a number of authors believe that the armed conflict, war in the board meaning, cannot be the main drive of innovation any more. They claim that innovations come largely from consumer-oriented industry branches and individuals can increasingly participate in and carry out technological innovations for security.

The talk about "democratization" of technology is more and more widespread, assigning it a new name: *peacetech*, which is to entail the spread and society's use of information and communication technologies for security. The technologies are supposed to allow satisfaction of specific, strictly defined needs by helping communities to live in safety and security. Social organizations such as Build Up or GICHD are emerging, with the goal of acting in this direction.

Build Up allows increased civic engagement in acting for security thanks to technology, arts and research. It cooperates with activists with various skills, including mediation or negotiation.

Through technologies it connects people involved in film making, design, coding, data analysis – all aimed at working for security. The Geneva International Centre for Humanitarian Demining (GICHD) is an expert organisation working to reduce the impact of mines, cluster munitions and other explosive hazards, in close partnership with organisations and other human security actors. These two sample entities: Build Up and GICHD aim to increase awareness about security through the possibilities of technological innovations. Thus, they are becoming effective administrators of technological innovations, offering possibilities to connect people to cooperate on solutions to security challenges and threats.

The potential of new technologies, in particular information and communication technologies – ICT, cannot be overestimated here. Hoverer, access to ICT remains highly uneven in developed and developing countries, affluent and poor ones. While 82 percent of people in developed countries use the Internet, in the global scale this percentage is merely 43 percent, 35 percent in developing countries, 11 percent in Africa and 9 percent in least-developed countries. The distribution of access to mobile phones looks slightly better, yet the prices of related services are the highest in the poorest countries. Without high-quality data providing information on security it is impossible today to design, monitor and assess effective security policies. In the end, technologies allow better understanding of the assessed phenomenon, enable decision-makers to follow the development of the situation and provide basis for corrective measures. Programmes already working for security by implementing information and telecommunication technologies allow the reduction of risks related to natural disasters, e.g. tsunamis. Mobiles phones and social media also create opportunities to strengthen actions for minimizing threats emitted by military conflicts. Photos and videos posted on social media in real time often become evidence for the scope and quality of violence (Larrauri, Kahl, 2013, p. 3). As a result, they may accelerate a government's or governments' response to the emerged seeds of conflicts.

These technologies have also revolutionized people's ability to organize and coordinate protest movements, from the Arab Spring to the war in Ukraine. This may have both positive and negative consequences. It needs to be remembered that technologies equally often cause increased invigilation and restriction of moral rights and easy manipulation of information and sources while a risk of their virus-like spreading without verification might promote disinformation. Social media users risk that they will find themselves in "information cocoons", where they encounter different opinions, which potentially enhances political polarization (Nagel, 2001, pp. 31–34.).

On the other hand, social media may also facilitate blocking and combating radical ideologies. Platforms such as Facebook may be used to boost positive interaction between people, often hostile against each other, through competitive political programmes, ideologies or ethnic or religious identity. Groups such as *Peace Factory* use Facebook to connect people in Israel with people in Iran, Palestine or Jordan, and groups such as *Umati* in Kenya or *Proxi* in Spain use social media to monitor and prevent hate speech. In Sudan, where the government had used technology to limit access to the Internet, a local NGO established a system of social connectivity which connects text messages with the radio in order to help maintain local agreements on normalization of life and increasing security. Video games teach war, but *Games for Peace* use Minecraft to gather youth from Israel and Palestine (Larrauri, Kahl, 2013, p. 6).

Information and communication technologies ensure possibilities to gather data on crisis situations and conflicts and narrow the gap between the emergence of a threat and a response. For instance, crisis monitoring or social media mapping may help in generating data on conflict indicators. Data generated by these tools may help authorities to take remedial measures. It may also better inform about the efforts for the prevention of conflict or monitor cases related to arms trading or violating human rights.

New technologies have changed the way wars are fought – there in no doubt about it today.

Similarly, processes of limiting and impeding them also have a great impact.

Particularly useful for peace operations are technologies that facilitate monitoring and observation, including drones (UUAVs), video monitoring systems, motion detectors, and satellite imagery. These devices can transmit and record images in order to disseminate them in a wider scale and for further analysis; images may also serve as evidence in cases of infringement of security. The listed technological solutions allow observation from a safe distance away from dangerous areas, therefore they are particularly useful for peace-guaranteeing forces (*The Impact...*, 2016, p. 8). They allow managing humanitarian convoys and provide precise information on the places where such aid may be effectively provided. These technologies can particularly help operations in the asymmetric threat environments in which it is increasingly not possible to act in any other way (Dorn, 2011). The war in Syria, its course and acting for security in this country excellently confirm the usefulness of these technologies.

New technologies also offer new possibilities of conflict management and creating security, especially at a local level. Apart from helping in preventing conflict, the tools for gathering and processing data may aid communities in coming out of situations of lack of security. The Intergovernmental Authority on Development (IGAD) in east Africa launched the ICT 4 Peace project as part of the mechanism of early warning and response in conflict situations (*The CEWARN...*, 2016).

New possibilities of using technologies do not concern actions taken in places of conflict, most often associated with remote and poor countries. The threat of terrorist attacks after the events in the United States and Europe has significantly changed the outlook on security issues, including the subject matter of using information and communication technologies in public space, in particular with reference to large metropolises and global cities. Not only was the presence of police forces increased significantly there, but also the most important buildings were surrounded by circles of barriers and fortifications. It was decided that places requiring attention in terms of security include all locations with large groups of people: squares and markets, stadiums or transport infrastructure facilities such as railway and subway stations. Protection and security in public space have undergone significant revitalization. The suggested or applied traditional space protection measures raise a number of doubts. Having provisions against threats on a global scale seems absurd, it is difficult to talk about areas to which access is blocked by metal detector gates combined with the necessity to undergo personal checks (Piątek, 2017, p. 82).

The proposed restrictions often raise objections, motivated by a restriction of civil freedoms and a threat of an attack on a free and open society. Streets and squares of the City of London even before announcing the global war on terrorism had been controlled and monitored by one of world’s largest and most advanced antiterrorist systems of security and visual surveillance, the so called “ring of steel”. The *Ring of Steel* was launched in July 1983 following a wave of bomb attacks carried out by the Irish Republican Army (IRA). The security cordon around the City was less visible than its prototype, erected in 1972, a steel ring of fortifications around Belfast’s central district. London streets were partitioned by steel cones and access lanes to checkpoints were marked with plastic cones. With time this entire system was named “ring of plastic”, however the presence of protection measures and police control were still widely felt. Plenty of drivers entering the city centre did not know the essence of the introduced security measures as their antiterrorist function was not publicly exposed. Quite the opposite, the introduced changes were explained to be measures aimed at limiting motor-vehicle traffic in the centre applied in order to facilitate road traffic and protect the natural environments. The system of antiterrorist regulations and security measures was officially called the Experimental Traffic Scheme. With time the area covered with protection expanded and now covers over 75% of the City. The protection of the area was reinforced by CCTV surveillance, both state – and privately-operated. The police forces initiated the *Camera Watch* action encouraging local traders and building owners to monitor video surveillance systems (CCTV – Close Circuit Television) in a coordinated manner so that the video surveillance also includes the city and streets in the vicinity of guarded private property. The most advanced system of cameras was installed in the points of controlled entrance to the City. In February 1997 a system of digital cameras was introduced, connected with the police data base (ANPR – *Automatic Number Plate Recording*), which is able to record automatically all number plates of cars entering the City, recognize suspicious numbers in 4 seconds and send out a return signal to checkpoints. In 2014 30,000 police cameras were operating in the centre of London, including many connected to the ANPR system, making London a city most saturated with these devices; a statistical Londoner is photographed daily by approximately 300 cameras (Rybarczyk, 2014). It is estimated that over 4 million cameras have been installed in the British Isles (Siergiej, 2010). Each video surveillance unit currently has two SONY FCB series high resolution camera modules. Images from the cameras are sent to the data centre of the Metropolitan Police in the New Scotland Yard. These are both colour and infrared images which the police analyze using the Talon ANPR software from NDI-RS that recognizes number plates. The received data is automatically compared with databases of other police delegations, Her Majesty's Revenues and Customs, the Driver and Vehicle Standard Agency and the UK Border Agency in order to detect potential threats as well as stolen, uninsured and untaxed vehicles.

According to the data from the Warsaw Centre of Monitoring Systems Management (ZOSM, *Zakład Obsługi Systemów Monitoringu*) there are 419 cameras in Warsaw and images provided by them go to, i.a., a special unit in the Warsaw City Police Department and are constantly viewed by the ZOSM's operators who report about ten thousand incidents to the police every year. Warsaw cameras are watched constantly, in contrast to British cameras which are observed at random and the recordings are checked only when a crime is committed in the observation field (Henzler, 2011).

In 2005 New York authorities took a decision about creating a similar system to the London one. In November 2008 a monitoring system was launched covering the southern edge of Manhattan. The Lower Manhattan Security Initiative, as it was called, covers an area of almost 5 square kilometers with its "overview". The beginnings were modest, 156 cameras and 30 mobile license plate recognition devices. However, since the beginning of 2011 over three thousand cameras have been following the behaviour of cars and pedestrians in Manhattan. It was also decided that the monitoring system will operate in real time, which means that images from cameras will be viewed directly in the command centre.

How to analyze images from so many cameras? How to single out information about potential danger from an avalanche of data? This exceeds perception capabilities of even several hundreds of supervising persons. The problem was solved by the introduction of smart software allowing image analysis.

The problem exists and does not only concern large agglomerations.

Increasingly, for many the ease of observation of suspected persons, and in the event of an assault – identification of the offender, is a guarantee of security. Persons responsible for the monitoring systems stress that the process is under control. However, a number of opponents of such an approach to the problem point out that monitoring is extremely dangerous since technology allows a lot. In 2008 South Korean police tested in the Seoul subway, in natural conditions, a face recognition system developed by a Californian company 3VR. The computer system was able to identify 9 out of 10 people in a fast moving crowd. Also here new opportunities are brought by the use of observation drones which raise the camera and video transmission equipment into the air. A drone, invisible against the sky, may follow a selected person for hours, flown by an operator sitting comfortably in an office chair. Instead of sending agents to the field, risking losing the figurehead or being recognized by the enemy, the drone hovers over the followed person and meticulously records all images seen. However, even an extensive system of cameras and surveillance operated by smart software has some limitations. An attack on the monitoring system may cause situations in which it will be beyond control. As a result of an attack a Hollywood scenario may materialize, in which cybercriminals deceive police officers sending them images presenting an alleged incident requiring urgent intervention (Donohue, 2016).

Technological expansion of the security environment may lead to the sense of greater security. However, we must be aware of the consequences. We are subject to a number of CCTV-related undertakings, we experience continuous following and our steps are recorded and analysed by a multi-level structure based on industrial television and visual surveillance (Minton, 2012).

The use of information and communication technologies is increasingly becoming a guarantee of security, thanks to the ease of observation of the suspected persons and in the event of an attack – the identification of the aggressor.

A British government programme *e-borders* required ten years of cooperation between specialists and cost over GBP 500 million. Its aim was to identify suspected persons during border checks. According to its originators, e-borders allows for early identification of people who could threaten security, e.g. those suspected of terrorism or other crimes who have been previously deported. Its full scope will be achieved after creating a complete monitoring system and the participation in it of all airlines (*Projekt*..., 2013).

CONCLUSION

In contemporary democracies there is an obvious divide between the governing and the governed; state on the one side, citizens on the other. There is professional politics and there are people dealing in politics only sporadically (if ever). There is a belief in the western civilization that the society must be involved in the operation of policy mechanisms (Tansey, 1997, p. 178). The purposefulness of measures taken in terms of creating a security policy "without a war" – "without violence" is doubtful. In today's multicultural world a far-reaching cooperation between different civilizations is therefore necessary. Anyway, the contemporary world, which in a sense has become a "global village", because of this only is already unified to a certain extent. Ryszard Kapuściński, however, noted that "(...) despite the progress in communication and connectivity, our mutual familiarity, despite the widespread myths, is still superficial, and most often non-existent. (...) we do not live in a global village, but rather in a global metropolis, at a global railway station or train stop, through which a lonely crowd (...) of troubled people who do not want to know each other or get closer is passing" (Kapuściński, 2002, p. 102). However, such an approach to security does not exempt us at all from caring to learn its limitations, even if we see them in the past. As long as we are not able to specify the sources of threats and to eliminate them, we will have to be aware that there are no conditions for security. The current wave of technological changes has created new possibilities of multifaceted cooperation in a wide range of areas, including sustainable development, conflict prevention, humanitarian responses, peacebuilding operations or state-society relations. At the same time, it has created new situations which are a challenge for the existing security-related norms.

BIBLIOGRAPHY:

Donohue, B. (2015). *Systemy kamer miejskiego monitoringu są dziurawe*. (10.06.2015). Downloaded from: https://plblog.kaspersky.com/systemy-kamer--miejskiego-monitoringu-sa-dziurawe/3047 .

Dorn, A. W. (2011). *Keeping Watch: Monitoring Technology and Innovation in UN Peace Operations*, Tokyo: United Nations University Press.

Dyczewski, L. (2008). *Terroryzm w mediach: sensacja i spektakl, odpowiedzialność i informacja*. Downloaded from: https://www.bbn.gov.pl/download/1/1979/zeszyt9dyczewski.pdf.

Henzler, M. (2011). *Kamery w miastach – wszędzie nas widzą*, (5.11. 2011). Downloaded from: https://www.polityka.pl/tygodnikpolityka/kraj/1518972,1,kamery-w-miastach---wszedzie-nas-widza.read.

Hoffman, F.(2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Kapuściński, R.(2002). *Lapidarium V*. Warszawa: Spółdzielnia Wydawnicza "Czytelnik".

Latiff, R. H.(2018). *Przyszła wojna. W obliczu nowego globalnego pola walki*. Warszawa: Wydawnictwo Naukowe PWN.

Minton, A. (2012). *CCTV increases people's sense of anxiety*, (30.11.2012). Downloaded from: www.theguardian.com/society/2012/oct/30/cctv-increases-peoples-sense-anxiety.

Nagel, T. (2002). *Concealment and exposure: and other essays*. New York: Oxford University Press.

Piątek, J. (2017). Poles in Great Britain. Dimensions of security after 2004. *Reality of Politics. Estimates-Comments-Forecasts*, 8.

Projekt ochronny kosztował miliony funtów. Wciąż nie działa (9.10. 2013). Downloaded from: http://www.polishexpress.co.uk/projekt-ochronny-kosztowal-miliony-funtow-wciaz-nie-dziala.

Puig Larrauri, H., Kahl, A. (2013). Technology for Peacebuilding. *Stability: International Journal of Security & Development*, 3.

Rybarczyk, M. (2014). *Londyn czeka na zamach*, (25.11.2014). Downloaded from: http://swiat.newsweek.pl/zagrozenie-terrorystyczne-w-londynie-i-na-wyspach-brytyjskich-newsweek,artykuly,352437,1.html.

Sachs, J. D. (2015). *The Age of Sustainable Development*, New York: Columbia University Press.

Siergiej, P. (2010). *Wielki brat na Manhattanie*, (6.01.2010). Downloaded from: http://wyborcza.pl/1,75476,7424790,Wielki_Brat_na_Manhattanie.html.

Tansey, S. D. (1997). *Nauki polityczne*, Poznań: Zysk i S-ka.

The CEWARN ICT 4 Peace Project: Use of Information Communication Technologies (ICTs) for Conflict Prevention, (1.04.2016), . Downloaded from: http://www.cewarn.org/index.php/the-cewarn-ict-4-peace-project-use-of-information-communication-technologies-icts-for-conflict-prevention.

The Impact of New Technologies on Peace, Security (2016). Development Independent Commission on Multilateralism (April 2016), Downloaded from: https://www.icm2016.org/IMG/pdf/new_tech_paper.pdf.

Yáñez, F. (2017). *The Goal is Industry 4.0: Technologies and Trends of the Fourth Industrial Revolution*, independently published.