The Role of Network Technologies in European Cybersecurity

URSZULA SOLER

Abstract The twentieth-century technological revolution changed nearly all spheres of human life. The changes are particularly evident in the domain of communication where network technologies (the internet, satellite communication, etc.), which accelerated the development of social communication in an unprecedented way by eliminating and marginalising the significance of geographical, political or cultural borders, have played a pivotal role. However, the need for their social assessment is being raised increasingly because, on the one hand, network technologies serve the daily lives of millions of people very well, whereas, on the other hand, by analogy, they are accessible to socially detrimental groups, e.g., terrorists, enabling them to perform extremely hostile activities. So, may their social assessment be unambiguous? Many research centres dealing mainly with tracking, analysing and assessing terrorist acts committed by various groups all over the world are emerging in the United States and Europe. Network technologies are, among other things, utilised to commit these acts and to track them. This paper is devoted to the social assessment of the role played by network technologies in European cybersecurity.

Keywords: • network technologies • modern technologies • terrorism • society • technology rating • technology assessment

CORRESPONDENCE ADDRESS: Urszula Soler, Ph.D., Associate Professor, The John Paul II Catholic University of Lublin, Social Sciencies Faculty, Al. Racławickie 14, 20-950 Lublin, Poland, e-mail: urszula.soler@gmail.com.

https://doi.org/10.4335/2022.2.3 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Twentieth-century technological changes influenced the development of industry and services, but most of all, modified human communication in an unprecedented way. For less than one hundred years, the speed of communication have multiplied to an extent that spatial distances are no longer important. The foundation of international companies employing people from different countries who "meet" and work with the use of modern communication technologies has become the standard of the 21st century. The tendency was accelerated yet again over the last two years by the outburst of the COVID-19 pandemic. Network technologies are technologies that, in the recent decades, have brought about a special revolution, also covering the social dimension. Their emergence and development have uniquely impacted social life bringing with them numerous alterations, not only to the domain of communication, but also to threats. Their potential is utilised by ordinary people, governments, non-governmental organisations or the world of business. However, it rapidly transpired that network technologies are not only a great social asset but may be detrimental to society too. Socially detrimental groups – the world of crime or broadly speaking, international terrorism – very quickly started to utilise these technologies due to having unlimited access to them. This article is dedicated to the social assessment of the role played by network technologies in cybersecurity in Europe and whether, in the background of terrorist attacks, the rating of network technologies may be socially unambiguous. The method applied in this article is based on the analysis of existing literature and network studies carried out by European cyberterrorism research organisations.

2 Theoretical aspects – definitions

The most important terms concerning network communication and terrorism, which also utilises communication, are defined in this subchapter.

The term *network technologies* appeared for the first time at the end of the 1990s due to the development of the communication potential of the internet. The emergence of the internet, in combination with new achievements in telecommunication and computer sciences, lead to another great technological transformation – a shift from dispersed, isolated microcomputers and supercomputers to wide informatisation by means of interconnected information-processing devices utilising various formats (Castells, 2007:63). As time went by, computer devices penetrated all possible spheres of life and activity: home, work, stores, entertainment, transport, etc. The devices, often mobile ones, were able to communicate with each other without using their operating systems. The basic technology, applications and data are stored on network servers and the computational intelligence is embedded in the network itself: the sites communicate with each other and utilise necessary software enabling them to connect any device to a universal computer network. The network logic embodied by the internet started to be applied in each domain of activity, each context and each electronically connectable place (The Economist, 1997).

Network technologies are often called information-communication technologies or ICTs. This is a wide concept encompassing all technical means used for the transmission of information. In other words, ICT corresponds to the application of digital technologies that help people to process and transmit information. The technologies have a large array of applications – from personal computers to PDAs (Personal Digital Assistant), from mobile to satellite phones or from faxes to robots. The demand for more advanced communication technologies lead to extensive development in the late 1970s. At that time, telecommunication engineers dreamt about one thing – the death of distance (Cairncross, 1997:118). Over time, the dream became a reality and technologies such as the internet or satellite phones have emerged.

Modern technology-based communication changed ordinary human lives to an extreme degree. It is said nowadays that we are living in a global village where information serves all. All of it happened due to the information and communication revolution. Information and communication technologies have definitely changed peoples' lives. People utilise them in social communication, education or business. Collaborative virtual environments (CVE) gave business people a lot of opportunities to expand their activities all over the world – in various geographical locations – and, at the same time, enabled them to maintain their headquarters in their natural place of work and life. Satellite telephones diminished the distance in interpersonal relations. Relationships among people living in different cities, countries, sometimes even continents, have become quite common and are no longer surprising for anybody. The dream of twentieth-century engineers about the death of distance became true, and the outburst of SARS-CoV-2 additionally accelerated or even forced the death of communication distance.

Terrorism and its younger sibling – cyberterrorism – are among the most controversial terms in the modern world. There is not one, universally accepted definition of terrorism, with governments of different countries and agencies fighting terrorism using their own definitions of terrorism. According to a study carried out in 2003 by Jeffrey Record from the US Army, there are over 100 definitions of terrorism. Their range encompasses 22 different definition elements in total (Record, 2003). The term became controversial due to the mixing of interests of various states and nations. The problem is reported, among others, by the United Nations Organisation. However, due to the conflict of interests among sovereign states that each time individually define which entity is a terrorist and which is a freedom-fighter, the Organisation is not able to decide on the definition of terrorism (Koechler). It often happens that in one state a person is considered a freedom fighter and a terrorist in another.

According to Todd Sandler and Walter Enders, terrorism is the threat of using violence or the premeditated use of violence by people or national groups to achieve political and social goals by intimidating a large group of recipients with direct victims (Sandler, Enders). According to the researchers, there are two basic components characterising each modern definition: the presence or the threat of violence and a political/societal

motive. Without violence or the threat of using it, terrorists are not able to influence political decisions made in response to their demands, and if a political/societal motive is missing, the act of violence is a crime and not an act of terrorism (Sandler, Enders). Yet another, simplified definition of terrorism is approved by the National Consortium for the Study of Terrorism and Responses to Terrorism – START at the U.S. Department of State. From their perspective, terrorism is the threat of using or the actual use of illegal force by non-state actors to achieve a political, economic, religious or social goal through fear, coercion or intimidation (the International Institute for Counter-Terrorism).

Cyberterrorism is a younger sibling of terrorism that appeared with the emergence of network technologies. Simply put, it is a marriage between technology and terrorism. This type of terrorism is directly linked to technological progress. The term itself was introduced following the rapid and uncontrolled development of technology. The term *cyberterrorism* is equally controversial as the term *terrorism* and there is not one universal definition of it. Some scientists argue that the use of computers or resources of information technologies to commit any act of terrorism justifies the use of the term *cyberterrorism*. Others claim that cyberterrorism is an abuse of information systems and databases, e.g., the hacking of databases of organisations and obtaining information for illegal purposes. One of the definitions is cited by Dorothy E. Denning. In her opinion, it is a convergence between terrorism and cyberspace. These are generally understood as illegal attacks or the threats of attacks on computers, networks and information stored there in order to intimidate or force a government or people to act upon demands and to achieve specific political or societal goals. Moreover, to classify an attack as cyberterrorism, it needs to be violent towards people or property or at least cause fearful damage. Therefore, these are attacks leading to death or injury, explosions, plane crashes, water pollution or serious economic losses. Heavy attacks on key infrastructure may or may not be acts of cyberterrorism, depending on their size and impact. Attacks disrupting insignificant services or burdensome in financial terms are not acts of cyberterrorism (Denning, 2000).

There is yet another term associated with cyberterrorism, i.e., *pure cyberterrorism*. It is also sometimes called *bloodless terrorism*. It refers to acts of terrorism that only happen in the virtual world. Bank intrusions are an example of this. Terrorist organisations need funds to conduct their activities in the real world, and thanks to modern online banking systems and the full set of internet financial services, they are able (through cyberterrorism) to steal money from banks and then use it to finance other terrorist activities. The idea was discussed in 1991 and presented in the report titled "Computers at Risk" prepared by the Board of the American Computer Science and Telecommunications. The authors of the report pointed to the danger resulting from the fact that state functioning is too highly dependent on computers. Computers control energy supplies, air communication and financial services. They are utilised to store important information, medical registries, penal registries, and are also used by business. And despite common social trust, they are exposed to terrorist attacks due to improper construction and insufficient quality control mechanisms. A modern thief is able to steal

more money using a computer than a pistol. According to these authors, a terrorist of the future may cause more harm using a keyboard than a bomb (the National Research Council, 1991). Unfortunately, these predictions have already turned out to be true.

3 Can the development of network technologies prove socially detrimental?

In this paragraph, the social usefulness, and potentially detrimental effects, of network technologies are discussed on the basis of examples of specific technologies.

By assumption, new technologies are always supposed to serve the greater good of society and people, but due to the lack of limitations and easy access, there is no guarantee that the technologies are always used in accordance with their intended purpose. Google Earth technology (a computer programme displaying satellite, aerial and panoramic images taken from street level, as well as various types of geographical and tourism information on a three-dimensional model of the globe), is one of many modern technologies utilised by scientists from various disciplines, which serves as an example. It is used, among other things, to create maps for measuring the susceptibility of the earth's surface to floods and earthquakes or other natural disasters. At the same time, however, the technology may also be used for killing hundreds of innocent people. An example is the use of it by terrorists involved in attacks in Mumbai, India in 2008 (The Washington Post).

Biometric tools, utilised mostly to control the access to protected premises or authorised users accessing specific data, programmes or devices (unauthorised attempts to access ATMs, personal computers, computer networks, mobile phones, home alarm systems, etc.) are socially useful and one of the most dynamically developing areas of telecommunication and information technologies. Some countries implemented biometric solutions for border control. They are successfully used, for instance, in airports in the United States and Australia. Australia decided to implement the *Smart Gate* face recognition system (Gamm, Sester, Reindl, 2013:45-50) operating in parallel with traditional points of passport control. Passport control with the use of a face reading device lasts only 6 seconds. France (face recognition) and Great Britain (human iris identification) also intend to implement biometric systems. The spread of the Wuhan virus has rapidly accelerated the development of biometric technologies. At the same time, however, terrorists improve the methods of passing by or falsifying the biometry (it is suffice to mention money counterfeiting).

Visual Surveillance – namely, the monitoring of behaviour and the habits of people to influence, direct and protect them (Lyon, 2007) is yet another example of network technologies. It may encompass distant observation by means of electronic devices (such as CCTV cameras) or capturing information sent via an electronic route (such as the internet or phone) (Minsky, Kurzweil, Mann, 2013:13-17). The system is utilised by governments for intelligence purposes, combating crime, the protection of processes, people, groups and crime investigation, to name a few. It is also used by criminal organisations for planning and committing crimes such as assaults or abductions.

Tracking of personal data, namely, obtaining personal information from various sources, comparing them and drawing up subsequent conclusions based on them in order to create a profile with the use of modern communication tools, is often utilised nowadays. The use of large sets of data may be very advantageous for businesses, governments and non-profit organisations. However, it is also stressed that, considering the rules of protection of data and privacy, the phenomenon of profiling should be limited to a necessary minimum. Informing users that they are subjects of profiling, even if it is carried out on the basis of commonly accessible sources, is also highly important. Various types of profiling are used to combat terrorism (Podniesienie skuteczności działań policji, 2010) (profiles based on specific intelligence information, profiles not based on specific intelligence information, profiling by "data exploration"), while it is ethnic profiling that has seen an increase in recent years. (It is nothing new in the Member States of the European Union. Its significance has increased in response to terrorist attacks in the United States (2001), Madrid (2004) and London (2005), and to growing concerns about illegal immigration). However, the use of ethnic profiling also raises concerns among intergovernmental organisations such as UNO, the Council of Europe and the European Union, as well as non-governmental organisations dealing with the protection of human rights. One argument that is cited particularly often is that ethnic profiling not only collides with the law on discrimination but also brings disadvantageous societal effects. In addition, terrorists often utilise false profiles to hide their true identities.

Reconnaissance satellites – often commonly referred to as spy satellites – are yet another, modern network technology. Their goal is to observe objects on the earth and capture signals from the earth for military or intelligence purposes. The observation is often linked with taking high-resolution photographs (up to below 1 m) that may be used in various ways (for example, to track the movement of enemy military troops or obtain information on potential targets on an enemy's territory). There are also satellites capable of obtaining information through clouds and at night, taking infrared photographs or using radar. Their basic goal is to provide data concerning the economic-military potential of a probable opponent, structures and equipment, as well as the location of an opponent's troops and the level of preparation for state defence (Nowacki, 2002:57-64). The Allied Forces operation, carried out by the forces of the North Atlantic Treaty Organisation (NATO) from 24 March and 20 June 1999 in the Federal Republic of Yugoslavia, aimed to put the ethnic cleansing in Kosovo to an end, to restore the multi-ethnic character of the province and to force the process of democratisation in Yugoslavia, is an example of satellite use. Aerial and space reconnaissance means were mostly used (Marszałek, 2009). During the operation, reconnaissance satellites (IMINT, Imagery Intelligence satellites, equipped with electro-optical apparatus and high-resolution infrared sensors (IR), Lacrosse satellites for radar imagining of the operation's area and ELINT/SIGINT satellites of the Mercury, Mentor, Trumpet and Orion type, assigned for capturing electronic signals in a wide range of frequency) mostly tracked the location of Serbian military forces and their communication, capturing radio signals and taking photographs of the enemy's military posts. In theory, satellites may not be used for unlawful purposes,

however, the practice proves otherwise. Like in the case of other technologies, satellites may be utilised by terrorists for the same purposes as military ones.

Computers and the internet are yet another examples of not so recent network technology that, on the one hand, is helping to combat terrorism but, on the other hand, is likely to serve terrorist purposes. Cyberterrorism was mentioned in the preceding paragraph while some more examples are discussed here. Computers were originally designed as computational machines, and in time, they became a medium utilised in nearly all spheres of human life. In combination with the internet (originally designed for the military in the form of the ARPANET network), their capabilities increased incalculably and are utilised for combating crime and terrorism, but also serve terrorism itself. It is suffice to mention bank account intrusion, illegal network transactions, and the Dark Web (Deep Web, Deepnet, Invisible Web, Hidden Web).

The Dark Web (Egan) is the term referring to a specific set of sites that are theoretically visible to all, but their IP addresses and host servers are hidden. It is a huge network of encrypted internet sites inaccessible through ordinary search engines (Wasiuta, 2019:251). To access them, one needs to use specially designed applications. Moreover, a skilful configuration of network settings is needed (Merriam-Webster.com). Nearly all sites of the Dark Web hide their identity using Tor, an encryption tool enabling the end-user to hide their identity and to falsify their location. To enter the Dark Web site encrypted with Tor, Tor needs to be used.

The Dark Web, called "the shady network", is a small proportion of the overall percentage of the Deep Web. The majority of sites encrypted on the Dark Web are typically amateur because it is easy to create a profile and win publicity there. The dark side of the internet is beyond the influence of the largest corporations dealing with technological development or media institutions. The Dark Web is constantly developing and the amount of money generated from transactions performed there remains immeasurable. It is strongly related to the first internet networks, such as ARPANET, due to the fact that both links are universally recognised under their shameful name as "a haven for illegal activities" (Beattie). The complexity of the operating schemes of search engines adjusted to surfing the Dark Web makes the reviewing of content very difficult and chaotic because the addresses of internet domains are almost constantly changing to ensure total non-detectability of their users. At first glance, the majority of sites resemble the ordinary internet that we use daily. However, they are differentiated by the fact that their names do not end with a classic .com or .pl, but with .onion (Stawska). Some people excessively use the Dark Web because anonymity helps them to commit various crimes – from paid killings to child pornography and stealing sensitive data such as personal photographs, medical records encompassing health condition information or documents proving the financial resources of private individuals (Beattie).

According to the Cambridge Dictionary, the Deep Web is "parts of the internet that cannot be found using ordinary search engines" (Cambridge Dictionary). It needs to be noted

that definitions of the Dark Web and Deep Web are similar to each other, but the Dark Web is only a small part isolated from the Deep Web. The size of the Deep Web is immeasurable. The Deep Web contains huge amounts of data and many various sites. The unindexed resources are inaccessible through popular search engines, but indexed sites may also be found there, but access to them is not as easy as in an ordinary internet network. The causes of the creation of the Deep Web include the forms of operation of the most popular search engines in the world, the lack of digital-information skills of network users and the fact that data providers utilise commercial and restrictive access (Cisek). It is highly important to understand the differences between the Dark Web and the Deep Web. Although the size of the Deep Web is immeasurable, in 2001 it was estimated to be approximately 400 to 500 times larger than Surface Web, namely the internet that is publicly accessible and used daily. On the other hand, the Dark Web incorporates a few thousand encrypted sites constituting 0.01% of the Deep Web.

The Silk Road and its descendants are examples of Dark Net sites. The Silk Road is utilised for buying and selling illegal drugs. However, there are also different applications of the Dark Web. Individuals operating in closed, totalitarian societies may use the Dark Internet to communicate with the outside world. Generally speaking, the Dark Internet mostly serves widely interpreted terrorism.

The list of crimes committed on the Dark Web is extensive. They are enumerated and discussed in detail by Shubhdeep Kaur and Sukhchandan Randhawa from the Thapar University in their work: *Dark Web: A Web of Crimes*. They presented a detailed list of the twelve main types of crime. These include illegal drug trade, human trafficking, the leaking of sensitive information, child pornography, proxying (a form of fraud, scam), the illegal sale of stolen debit and ATM cards, fraud in the domain of Bitcoin (a currency used by network users, also including cybercriminals), illegal weapon trade, "onion cloning" (the redirecting of a user to a false link to convince the user that the site is original; it is related to the stealing of money), contract killings, red rooms (paid, live streams of murders, rapes, tortures, child pornography, etc.) (Kaur, Randhawa, 2020).

Mobile and satellite phones (communication, detonation, etc.), television (mainly used as a form of communication and intimidation – demonstrative decapitations, etc.) and other already-mentioned modern inventions may also serve cyberterrorism. Sometimes, the facilitation of terrorist attacks results from indiscretion and insufficient knowledge of people using a specific technology. Suffice to mention the case from 2018, when the American CIA base in Mogadishu and the Russian air force base in Syria, both secret military facilities, were located based on a map made available through the Strava sports application.

In recent years criminals have started to successfully utilise social media. Even the term *Twitter terrorism* (BBC News) appeared. It is assumed that the Islamic State owns over 50 thousand accounts on Twitter, utilised mostly for communication. Steganography (the communication science that teaches people how to communicate in order to protect

communication against detection) is also commonly utilised. With the use of it, a hidden message is concealed within different content that does not look like a hidden message. Photographs, millions of which may be found on the network, are often utilised for this purpose.

4 Organisations researching the increasing (cyber)terrorism

There are many various organisations researching terrorism and the impact of modern technologies on terrorism all over the world. The studies are conducted mainly to understand how new technologies may be protected against abuse. Only a few of them shall be enumerated here: in Israel – the International Institute for Counter-Terrorism, in the United States – the Office of the Coordinator for Counterterrorism at the U.S. Department of State and START – the Study of Terrorism and Responses to Terrorism – the national consortium of the U.S. Department of State and the University of Maryland. The SAFETY Act (the Support Anti-Terrorism by Fostering Effective Technologies Act) (Cellucci, Davidson, 2011) is also important – the programme adopted in 2002 by the American Congress in response to the attacks of 11 September 2001. In Asia, SATP (South Asia Terrorism Portal) – an organisation researching terrorism and focusing, in particular, on South Asia, has been operating for years.

In addition, more and more research centres dealing with cyberterrorism are being established in European states. ITSTIME – the Italian Team for Security, Terroristic Issues & Managing Emergencies of the Catholic University of the Sacred Heart in Milan – is one of the most interesting. The team, coordinated by Prof. Marco Lombardi, is composed of experts in various fields and competencies. ITSTIME deals with new challenges in the new domain of hybrid war from a theoretical and empirical perspective, focusing mainly on security interpreted as a condition resulting from the establishment and maintenance of protective means capable of promoting the well-being of citizens and the democratic vitality of institutions and terrorism as a long-term risk which needs to be combated by means of well-designed preventive measures and crisis management to develop practices useful for citizens and institutions (ITSTIME).

KCL Cybersecurity Centre operates in London. It is an academic excellence centre operating in the field of research on cybersecurity EPSRC-NCSC (ACE-CSR). It gathers scientists from King's College London dealing with the socio-technical aspects of cybersecurity, including scientists from the Department of Informatics, War Studies, Defence Studies, Digital Humanities and the Policy Institute. Many scientists working over the three main research themes and their interrelations, namely: AI Cyber Security, Formal Cyber Security and Strategic Cyber Security, collaborate with the Centre. The purpose of the Centre is to deliver research to inform about and implement innovations (KCL).

The Cyber Security Academy based in Hague focuses on the development of professional education in the broad sense of cybersecurity in collaboration with LDE universities and

the Hague University of Applied Science. CSA is an initiative of Leiden University, Delft Technical University and the University of Applied Sciences in Hague. The Center for Law and Digital Technologies (eLaw) offers post-gradual studies to professionals working on the organisation of (cyber)security in the private and public sectors (CSA). The Centre examines the social, legal and normative impacts of emerging digital technologies. In the research and education that is conducted, the Centre focuses mainly on digital technologies and their interrelations with basic law and governance.

INIS (The Institute for National and International Security) also plays an important role in the research on cyberterrorism in Europe. INIS is a Scientific Academic Society (recognised by the government of Serbia) promoting security sciences and publishing the "Security Science Journal". And at the same time, it was the first institute in the world that started the analyses of security as a science. INIS gathers academic staff, researchers and scholars to share information and expertise through research papers, situation reports and academic publications for worldwide distribution. It is worth mentioning that INIS administers the largest public domain research database on terrorism and organised crime. The TOC-search (the Terrorist Organised Criminal Search Database) is a dynamic database offering comprehensive information on global terrorist networks and helping researchers, analysts, students and others to prevent terrorism. The INIS mission is to organise and conduct academic and scientific-research activities in the field of national and international security either individually or in collaboration with other, higher education and scientific-research institutions, state bodies, public institutions, enterprises, and civil society organisations.

A young but rapidly developing Polish think-tank is also worth mentioning – the Academic Centre for Cybersecurity Policy (ACCP), operating at the War Studies University in Warsaw whose main goals include, in particular, the preparation of analytical papers (analyses and expert opinions), reports, recommendations and thesis-information materials in the domain of cybersecurity with particular consideration of legal aspects, for the purposes of the Ministry of National Defence, including managerial staff and other entities dealing with cybersecurity in the Republic of Poland. The Information Security Lab is a part of the Centre conducting, among other things, research on cyber-surveillance, cybercrime, cyberterrorism and cyberwar. The Centre also publishes an academic journal titled "The Cybersecurity and Law Journal".

5 Summary

(Cyber)terrorism utilising network technologies is still growing while, at the same time, more and more centres combating it are being established. Information and communication technologies influence every human being and each domain of life. By simplifying communication, the technologies have made our lives easier. However, some new, previously unknown threats have also emerged. The last twenty years have brought about huge transformations in the world of technology. The most vivid example of this is the evolution of the mobile phone that, at the beginning of the nineties, was considered a

luxury, and today, people use PDA equipment as a tool facilitating communication in nearly each and every process of communication. The transformation, referred to by some authors as "technology development" was an incentive for an economic race among countries and organisations. However, it has also become an incentive for a race among the world of crime and those who fight it. So, are network technologies socially useful? The answer is not as easy as it seems. While, on the one hand, the answer is definitely affirmative, on the other, network technologies are a source of serious risks connected with the fact that they are utilised by unauthorised people in an improper way. Nevertheless, the dilemma has been true in the case of each type of technology since its onset. The social rating of technologies is not easy but it is needed because technological development, accompanied by social development, does not necessarily or always have to serve the greater good of society.

References:

Bjørgo, T. (2005) *Root causes of terrorism: myths, reality and ways forward* (London, New York: Routledge).

Castells, M. (2007) *Społeczeństwo sieci* (Warszawa: PWN).

Cairncross, F. (1997) *The Death of Distance: How the Communications Revolution Will Change Our Lives* (Boston, MA: Harvard Business School Press).

Cellucci, T.A. & Davidson, B. (2011) *SAFETY Act: Adding Value through Strategic Deployment* (U.S. Department of Homeland Security).

Denning, D. (2000) *"Cyberterrorism", Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services* (US House of Representatives).

Gamm, G.U., Sester, S. & Reindl, L. (2013) SmartGate - Connecting wireless sensor nodes to the Internet, *Journal of Sensors and Sensor Systems*, 2(1), pp. 45-50.

Koechler, H. (2002) *The United Nations, the international rule of law and terrorism*, Fourteenth Centennial Lecture, Supreme Court of the Philippines & Philippine Judicial Academy, available at: http://hanskoechler.com/koechler-IRLUN-Berlin-Jan05.htm (August 30, 2022).

Kosikowski, C. (2016) Nowe Prawo rynku finansowego Unii Europejskiej, In: Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warszawa: Wolters Kluwer), pp. 27-38.

Lyon, D. (2007) *Surveillance Studies: An Overview* (Cambridge: Polity Press).

Marszałek, M. (2009) *Sojusznicza operacja "Allied Force": przebieg - ocena – wnioski* (Toruń: Wydawnictwo Adam Marszałek).

Minsky, M., Kurzweil, R. & Mann, S. (2013) *The Society of Intelligent Veillance*, Proceedings of the IEEE ISTAS 2013 (Toronto, Ontario, Canada), pp. 13-17.

National Research Council (1991) *Computers at Risk* (Washington, DC: National Academy Press).

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M. & Gagnon, G. (1999) *Cyberterror. Prospects and Implications*, White paper, available at: https://calhoun.nps.edu/bitstream/handle/10945/27344/Cyberterror%20Prospects%20and%20Implications.pdf?sequence=1&isAllowed=y (August 30, 2022).

Nowacki, G. (2002) *Rozpoznanie satelitarne USA i Federacji Rosyjskiej* (Warszawa: Akademia Obrony Narodowej).

FRA (2010) *Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu: przewodnik* (Luksemburg: Urząd Publikacji Unii Europejskiej).

Record, J. (2003) *Bounding the global war on Terrorism* (Strategic Studies Institute).
Sandler, T. & Enders W. (2011) *The Political Economy of Terrorism* (Cambridge: Cambridge University Press).
Wasiuta, O. (2019) Dark Web, In: Wasiuta, O. & Klepka, R. (eds.) *Vademecum bezpieczeństwa informacyjnego* (Kraków: Instytut Nauk o Bezpieczeństwie, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej), pp. 251-256.

.