Politeja
No. 6(69), 2020, pp. 183-196
https://doi.org/10.12797/Politeja.17.2020.69.09

Dominika DZIWISZ
Jagiellonian University
dominika.dziwisz@uj.edu.pl

POSSIBILITIES OF APPLYING THE CHINESE SOCIAL CREDIT SYSTEM TO COMBAT TERRORISM

ABSTRACT 2011 saw the start of the pilot phase of the Social Credit System. The societies of democratic states interpreted it as an extreme example of human rights violation. In turn, what is usually forgotten is that the SCS is not the first citizen assessment system, because similar systems have been successfully functioning since 1960s in democratic countries. Scientific analyses of SCS operations are usually limited to its negative consequences. There are fewer attempts by governments of democratic states to assess the use of elements of SCS and algorithmic data analysis, for example in order to increase the level of security of citizens. As a result, this article presents the research hypothesis that elements of the SCS may be successfully applied also in democratic states for the purpose of more effective combating of terrorism. With modern methods of analyzing Big Data sets, it is possible, for example, to accelerate recognition of terrorist networks, support identification of sources of radicalization in online communities and increase the effectiveness of anti-terrorist strategies in order to protect citizens against contemporary terrorist threats. For such a system to be as effective as possible, it should take over some assumptions of the SCS which are explained in this article: Firstly, it should be centralized and controlled by the state. Secondly, the information obtained and processed should be used solely for the purposes of the state security policy, i.e. in the scope smaller than in the case of China. Thirdly, the data should be obtained from multiple sources, public and private ones, in order to increase the accuracy of predictions. Fourthly, the violation of the principles of social coexistence might result in specific penalties, and compliance therewith – in rewards.

Keywords: Social Credit System, terrorism, international security, Big Data, China

INTRODUCTION

In the year 2000, the Politburo of the Chinese Communist Party decided that development of an advanced information society was going to be one of the key political objectives for the coming years. That decision was based on the conviction that the Internet and social media would allow the Chinese government to improve the standards of state management while preventing social discontent. The statement of President Jiang Zemin at an international IT conference in Beijing was clear evidence that the communist government of China was noticing the benefits of providing citizens with the Internet despite the fears that unlimited dissemination of knowledge and ideas might challenge the principles of functioning of the society.[1] At the same time, it was an implicit declaration of belief in the possibilities of using modern technologies to increase control over the society.

In the very same year, proper institutional changes were implemented, among others: there was established the State Council Information Office (SCIO), China's Computer Emergency Response Team, as well as the Internet Society of China, a non-government organization of representatives of the Chinese online industry, supported by the Chinese authorities. Two years later, in 2002, the Political Report presented by the secretary general included the first remarks about development of the system for IT mass surveillance – the Social Credit System (SCS).[2] Based on the initial announcements, the System was to support development of the emerging Chinese market economy, and trust was considered a key element of supporting market transactions. In turn, apart from information on the creditworthiness of clients, reported by banks and other financial institutions,[3] the central government would also receive non-financial information, both positive and negative, such as data from courts, telecommunications operators, fiscal administration units, government departments, etc. American political scientist Deborah Seligsohn has noted that the fundamental problem of management for every authoritarian regime boils down to obtaining credible and compete information on what is happening at the lower levels of administration.[4] In a state with 1/5 of the world's population and a developed economy, but without public debate, civil society or feedback from voters, it is not easy to obtain credible information on the behavior of

[1] M. Jussawalla, R. Taylor, *Information Technology Parks of the Asia Pacific: Lessons for the Regional Digital Divide*, London, 2003, p. 264; N. Inkster, *China's Cyber Power*, London 2016, pp. 23-24.

[2] R. Creemers, „China's Social Credit System: An Evolving Practice of Control", *SSRN Electronic Journal*, 9 May 2018, at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792>, 8 May 2019.

[3] C. Zhou, *Credit Information Database in China*, conference paper, Kuala Lumpur, 5-9 November 2012, at <https://www.ifc.org/wps/wcm/connect/e722b080438c5bc481f5b9869243d457/Session_8_C.Zhou_credit+database+in+China.pdf?MOD=AJPERES>, 10 July 2018.

[4] C. Larson, "Who Needs Democracy When You Have Data?", *MIT Technology Review*, 20 August 2018, at <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>, 12 January 2020.

people at the local level. In 2002-2012, during the presidency of Hu Jintao, an attempt was made to handle that problem by allowing a modest democratic thaw. President Xi Jinping reversed that trend and ordered the largest program of algorithm-based surveillance. In other words, he started to use information technology, artificial intelligence, and Big Data analysis to monitor even the minute elements of the lives and behaviors of 1.3 billion citizens.[5]

The year 2011 saw the start of the pilot phase of the Social Credit System. Democratic states around the world interpreted it as an extreme example of human rights violation including, in particular, the right to privacy. In turn, what is usually forgotten is that the SCS is not the first citizen assessment system, because similar systems have been successfully functioning since 1960s in democratic countries as well. Nowadays, data brokers, such as Experian, monitor whether clients' debts are repaid in a timely manner, by assigning points which are then verified by lenders, eBay customers can evaluate shipment time and communication, Uber drivers and passengers evaluate each other, and 70 per cent of employers monitor the social media activity of job applicants before making the decision on whether to employ them.[6] The Chinese SCS takes a step further and expands that idea to all aspects of life, assessing, in an aggregated manner, the behavior and credibility of citizens by monitoring each manifestation of activity of natural persons and businesses.

Scientific analyses of SCS operations are usually limited to its negative consequences. There are fewer attempts by governments of democratic states to assess the use of the elements of SCS and algorithmic data analysis, for example, in order to increase the level of security of citizens against crime or terrorist attacks. It is worth noting the general shift of attitudes of governments towards their citizens. They make use of new technologies to provide citizens with more safety which, unfortunately, also results in limitation of civil rights and liberties. It seems that the process is unstoppable.

As a result, this article presents the research hypothesis that elements of the Chinese citizen surveillance system may be successfully applied also in democratic states for the purpose of combatting terrorism more effectively. With modern methods of analyzing Big Data sets, it is possible, for example, to accelerate recognition of terrorist networks, support identification of sources of radicalization in online communities, and increase the effectiveness of anti-terrorist strategies to protect citizens against contemporary terrorist threats.[7] For such a system to be as effective as possible, it should go over some assumptions of the SCS.

First, it should be centralized and controlled by the state. Participation of private enterprises is necessary only in order to obtain the most exhaustive information on threats. However, central control by state authorities is required to ensure security of

[5] Ibid.

[6] L. Salm, „70% of Employers are Snooping Candidates' Social Media Profiles", *CareerBuilder*, 15 June 2017, at <https://www.careerbuilder.com/advice/social-media-survey-2017>, 8 May 2019.

[7] *Global Terrorism Index 2017. Measuring and Understanding the Impact of Terrorism*, Institute for Economics and Peace, at <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf>, 8 May 2019.

the information transferred. Private companies and state governments usually have different motivations. Their ultimate objective is profit, while the objective of a state is to maximize the level of safety of its citizens.

Second, the information obtained and processed should be used solely for the purposes of state security i.e., the scope is smaller than in the case of China.

Third, the data should be obtained from multiple sources, public and private, in order to increase the accuracy of predictions. The most important change brought about by the digital age is that our activities do not have to be limited to small sets of data, which was necessitated by insufficient technology – now we can make use of all the existing data.

Fourth, the most controversial aspect is that violation of the principles of social coexistence might result in specific penalties, and compliance therewith – in rewards.

The cut-off date of the actual and legal status of the facts and considerations discussed in the article is December 1, 2019.

BIG DATA PREDICTIVE ANALYTICS IN FIGHTING CRIME AND TERRORISM

As stated above, the practices of democratic states include many key elements of the Social Credit System. What makes the SCS different from Western systems is the comprehensive, institutionalized assessment of citizens for the purposes of the state, which provides grounds for making various decisions, for example, issuing passports or granting the right to stay in certain countries. Furthermore, in Western democracies the data on citizens usually serves one objective i.e., assessment of creditworthiness, and come from few sources. With the central database, the Chinese system is capable of aggregating data from multiple sources, state and private, and use it in countless ways which ultimately contributes to enforcement of state policies. This means that the borderlines between data collection and analysis for commercial and state purposes overlap. Martin Chorzempa from the Peterson Institute for International Economics stated: *No government has a more ambitious and far-reaching plan to harness the power of data to change the way it governs than the Chinese government*.[8]

Big Data analysis is usually applied by democratic states on a smaller scale, for example, that of a district, city or larger administrative unit, by courts and law enforcement authorities. For example, an analysis performed using algorithms is applied by US parole boards in most states. When making the decision on whether someone is going to leave the prison earlier or service the entire sentence, predictions based on computer data analysis are taken into account. COMPAS is popular software, developed by Northpointe, and applied by US courts when making decisions on penalties, particularly in the states of Wisconsin, Michigan, and Florida, which takes account such factors as: criminal involvement, lifestyle, personality/attitude, or origin. In most

[8] C. Larson, *Who Needs Democracy…*

American states, Big Data analysis is used to prevent crimes by diagnosing who may commit them. Some cities use so-called 'predictive policing' i.e., the method of indicating the places where crimes can take place or the persons who are potential perpetrators. For example, the Blue CRUSH (Crime Reduction Utilizing Statistical History) system applied in Memphis, which indicates the most dangerous areas as well as times during which most police patrols should be sent there, contributed to a reduction in the level of crime by 25 per cent.

The interest in algorithmic data analysis on a national or international scale increased as a result of the demand for more effective intelligence and surveillance products after the controversy related to the activity of the US intelligence before the 9/11 attacks which failed to process specific information indicating a terrorist plot, but also after wrong information and decisions regarding the program of weapons of mass destruction in Iraq in 2002 employed to justify US intervention.[9] These events, among others, challenged the intelligence capacity of the US, particularly its Human Intelligence (HUMINT) capacity. People realized that intelligence techniques had to be adapted to a more complex security environment. As a result, American intelligence agencies started to apply systematic and sophisticated techniques of data collection and analysis.

Currently, algorithm processing of Big Data is applied by the largest intelligence agencies, particularly in predictive analytics (the terms data mining and data science are also applied, even though their scope is broader) i.e., the process of analyzing information in order to discover patterns in big data sets and predict future events. One of the main properties of Big Data is discovery of patterns and correlations in the 'information dump' to allow better understanding of the studied phenomenon. Unlike a dozen or so years ago, when information was collected for a particular purpose, not just in case, as it may prove useful in the future.[10] It may be used to predict future threats and make better use of the limited resources in order to better concentrate on the most direct threats. For example, predictive technologies may help in preventing future terrorist attacks by analyzing patterns from the previous attacks, for example, to indicate the locations where a terrorist attack may potentially take place. Such projections are nothing new in fighting terrorism. Intelligence agencies have been analyzing so-called Big Data for decades, by compiling various pieces of information for the purposes of comprehensive assessment of current threats. However, modern technologies allow analysts to aggregate unprecedented amounts of data and to notice trends, which used to be too time-consuming and not economical.

Predictive technologies may come in different forms. Predictions may be based, for example, on popular social media such as Twitter, which is often used by terrorists for recruitment. Analysts from the Qatar Computing Research Institute in Doha developed the algorithm which indicates, with 87 per cent effectiveness (according to them),

[9] D. Van Puyvelde, S. Coulthart, M. Shahriar Hossain, "Beyond the Buzzword: Big Data and National Security Decision-making", *International Affairs*, vol. 93, no. 6 (2017), pp. 1397–1416.

[10] K. Cukier, V. Mayer-Schonberger, *Big data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2014.

the Twitter users more susceptible to terrorist ideologies.[11] By following the tweets in Arabic generated by the persons who support ISIS and those who are against it, the characteristics of members of both groups were specified. Then, the history of tweets of each person was searched to find out whether their previous tweets from before the advent of the ISIS have any common factors which might determine their future behaviors, including support for terrorists or lack thereof. As a result, some uncharacteristic trends were discovered, such as the fact that ISIS supporters usually use its full name i.e., Islamic State of Iraq and the Levant. In turn, the persons that do not support ISIS use the abbreviated name. Another source of information on supporting or not supporting ISIS was hashtags i.e., the words or phrases preceded by the # (hash) symbol – a marker used for grouping messages. For example, the persons against terrorist activities hashtagged the events associated with supporting other rebel groups, mainly in Syria, which were attacked by ISIS.[12]

An example of one of the biggest databases on terrorist attacks is Dfuze, created by Intelligent Software Solutions (ISS).[13] The software was used, among others, to study the bomb attacks in Boston in April 2013, as well during the 2012 London Olympics, when more police patrols were sent to the places indicated as being at risk of a potential attack. Dfuze operates by analyzing previous terrorist attacks and explosives used to draw conclusions on where a terrorist attack may take place in the future. In other words, it forecloses decisions on increasing security in the potentially dangerous areas. The system is not 100-per cent effective, but it saves time spent on tedious data analysis, and is used in ca. 40 countries.[14] Similar tools for tracking potential sites of future terrorist attacks were developed by the PredictifyMe company. One of its products is Soothsayer – a software that predicts terrorist activities in Pakistan, Afghanistan, and Iraq on the basis of the 'Terror Migration' algorithm. According to its authors, its effectiveness is 72 per cent. PredictifyMe uses as many as 200 indicators, such as state holidays, weather, terrorist attacks in the countries nearby, sports events, and even videos on YouTube, to predict whether and when a terrorist attack may take place.[15]

The activities based on predictive analytics are included in strategic documents of many countries, such as the British counter-terrorism strategy (CONTEST) of June 2018.[16] British minister of internal affairs, Sajid Javid, announced that the strategy plac-

[11] C. Larson, "Twitter Data Mining Reveals the Origins of Support for Islamic State", *MIT Technology Review*, 23 March 2015, at <https://www.technologyreview.com/s/536061/twitter-data-mining-reveals-the-origins-of-support-for-islamic-state/>, 5 May 2019.

[12] Ibid.

[13] G. Peters, "Counterterrorism: Trying to Predict the Future", *Army Technology*, 16 September 2015, at <https://www.army-technology.com/features/featurecounterterrorism-trying-to-predict-the-future-4654343/>, 5 May 2019.

[14] Ibid.

[15] Ibid.

[16] *CONTEST The United Kingdom's Strategy for Countering Terrorism*, June 2018, at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf>, 10 May 2019.

es emphasis on use of technologies and provision of information on the persons that are observed by intelligence services for counter-terrorism purposes.[17] The strategy includes the activities divided into four categories, 'four P's': Prevent, Pursue, Protect, and Prepare, which boils down to protecting people from becoming terrorists or terrorism supporters, preventing terrorist attacks in Great Britain and abroad, supporting security against terrorist attacks in Great Britain and abroad, and limiting the effects of the terrorist incidents that actually take place. Each of these working categories limits the element of terrorism-related risks, and together they provide a sustainable and comprehensive response to threats.

The 'Prevent' objective is identification, at an early stage, of the persons who may be interested in potentially hostile ideologies and support terrorists, and support for recovering the persons already engaged in terrorism. Such conduct resembles the fight with city gangs, drug abuse or physical and sexual abuse. If there are justified premises that the given person will take a risky and dangerous path of development, that path may be altered through medical, pedagogical, and social assistance. In other words, by detecting hostile behaviors at an early stage, one can manage the risk posed by those persons, before they potentially reach the level in which they consider acts of terrorism.[18] The initiatives that are similar to the British ones include Five Eyes (USA, Canada, Australia, and New Zealand), or the European Union counter-terrorism strategy.[19]

OTHER APPLICATIONS OF BIG DATA TO FIGHTING CRIME AND TERRORISM

Algorithm-based data analysis is applied not only in predictive activities, but also at the stage of identification of intelligence targets i.e., recognition of general trends and anomalies, data collection, processing and analysis, and dissemination of intelligence information.[20]

The sudden development of the possibilities of collecting intelligence data through indexing mechanisms and data summary algorithms, which automatically identify, categorize, and store proper data, provided intelligence agencies with more analysis capacities. The new challenge is interpretation of the data available in the online public domain and differentiating between credible information and misinformation or propaganda. Such differentiation is possible with the so-called screening algorithms. However, sometimes it is difficult to identify or study credibility of the source of

[17] *Home Secretary Announces New Counter-terrorism Strategy*, 4 June 2018, at <https://www.gov.uk/government/speeches/home-secretary-announces-new-counter-terrorism-strategy>, 14 June 2019.

[18] *Using Big Data Effectively in the Fight Against Terrorism*, Defence Contracts Online, at <https://www.contracts.mod.uk/do-features-and-articles/using-big-data-effectively-in-the-fight-against-terrorism/>, 5 May 2019.

[19] Ibid.; *Home Secretary...*

[20] D. Van Puyvelde, S. Coulthart, M. Shahriar Hossain, "Beyond the Buzzword...".

information or contents of articles, and commonly applicable algorithms do not yet contain the functionalities that would allow to differentiate between them. That is why it would be a mistake to resign from old intelligence techniques, because human intervention is still necessary to identify the discriminating properties of false messages and to properly adapt algorithms. Within that context, Big Data does not change the character of intelligence activities, but only reinforces some of its traditional tasks, such as identification of what should be collected or ignored.

Big Data algorithms also help to process raw data into useful information. For example, the Taranis drone produced by BAE Systems is equipped with the sensors that can collect many types of data to identify threats and warn against dangers.[21] One can similarly recognize patterns and detect trends in larger data sets which, for example, will indicate growing instability in the given region of the world. What is more, information technologies are advanced enough for natural language processing (NLP). By combining the capacity of artificial intelligence and linguistics, one can automate the analysis, understanding, translation, and generation of natural language by a computer. The information recorded in the database is converted into the language readable and understandable by people. Modern applications may also facilitate the access for analysts to large amounts of data using visual aids. One example is the Geofeedia software i.e., the intelligence platform used by the US NSA that provides analysts with access to contents of social media in real time on the basis of location. An analyst's task is to contextualize the search results.[22]

Algorithms are also applied to data analysis i.e., to use the collected knowledge to make decisions.[23] Traditionally, at that stage the question that is asked is 'why' the studied trend or phenomenon occurs. Currently, hypotheses and searches for the answers 'why' are being replaced by looking for the answer to the question 'what'. This means that analysts limit their work to finding correlations instead of understanding the in-depth cause of phenomena. Even if the research results may sometimes seem illogical, statistically speaking correlation analysis provides positive results.[24] Computers do not think like people and probably never will, but they apply mathematics to analyze correlations and calculate the probability of occurrence of the given event. However, this does not mean that computers may be completely trusted and that one can resign from setting hypotheses and study causality.

Computers and algorithms are also used for disseminating intelligence information.[25] Apart from traditional, periodic reports, one can use, for example, a recommendation system that filters information and strives to predict the given user's 'assessment

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] D. Dziwisz, "Algorytmiczna przyszłość – ucieczka od wolności ku 'opcji domyślnej'", in P. Szymczyk, K. Maciąg (eds.), *Człowiek a technologia cyfrowa – przegląd aktualnych doniesień*, Lublin 2018, pp. 56-57.

[25] D. Van Puyvelde, S. Coulthart, M. Shahriar Hossain, "Beyond the Buzzword...".

of' or 'preference for' the given thing. Although such tools are usually used for commercial purposes, the report by Gregory Treverton indicates that similar applications are used by the American intelligence community.[26] For example, the US developed its own internal network of social media called eChirp, based on Twitter. It allows analysts to concentrate on the latest news from multiple agencies, just like Twitter does in the public area. If an analyst sends a question by Echirp about the situation in the given state, she will receive simultaneous feedback from many agencies. Big Data applications are also used to develop visualizations, for example, in the form of interactive maps tracking the changing frontlines during the conflict in Syria. A tool developed by Palantir documents over 70,000 conflict events and demonstrates the changing situation. As a result, analysts develop awareness of the situation and better analyze the information that is presented in a convenient manner.

CONDITIONS FOR SUCCESS OR FAILURE OF ALGORITHMS APPLICATION IN INTELLIGENCE ACTIVITIES

As elements of mass electronic surveillance are successfully used by intelligence services of democratic countries, it should be assumed that the temptation to develop an institutionalized system modeled after the Chinese one, is strong. It would mean constructing a centrally managed system, controlled by an institution established specifically for that purpose for evaluating citizens. Such a central information base would collect data from many sources, state and private, for the purposes of realizing objectives of national security. Probably, unlike in China, such a system could be developed with the consent of all the citizens of the given state, given in a referendum, to allow better counter-terrorism measure, at the cost of limitating civil rights and freedoms. The effectiveness of such a system will depend on multiple factors.

First, data analysis is effective only if performed almost in real time. With the gigantic amounts of data, collected all the time, on potential terrorist behaviors, data analysis constitutes a challenge for analysts from intelligence services.

Second, the data should originate from as many different sources as possible and cover, for example, participating in suspicious online conversations, contacting persons of extremist nature, withdrawing from main activities and events, travelling to conflict zones, and non-typical shopping.

Third, unlike the SCS, the obtained data may be used and processed solely for the purpose of executing the national security policy. Expansion of the catalogue of potential applications would lead to development of the climate of fear, like in China.

Fourth, as indicated by the research conducted by scientists from the Massachusetts Institute of Technology and PEN America, the awareness of being monitored

[26] Ibid.; G.F. Treverton, "New Tools for Collaboration. The Experience of the U.S. Intelligence Community", *CSIS*, January 2016, at <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160111_treverton_newtools_web.pdf>, 1 May 2019.

significantly affects our online behaviors.[27] For example, before secret information on surveillance of US citizens was published by Edward Snowden, intelligence activities were more effective in combating terrorism, because those planning the attacks were not aware that they were being monitored. That is why, without considering the potential consequences of their behaviors, they would search online for such terms as Al-Qaida or car bombs. After 2013, the situation has changed, because those planning the attacks have been more cautious and, as a result, the intelligence agencies were not capable of accurately predicting their future behaviors. The Chinese systems is based on completely different principles because it is visible, ubiquitous, and applies a system of penalties and rewards. Out of concern for sanctions, Chinese citizens are usually passive and do nothing that could in any way negatively affect their score. The conclusion is that if the governments of democratic countries do not change their policies to resemble the Chinese system (and let's hope they do not!), they will have to hide their operations and surveillance programs in order to fight the security risks more effectively.

Fifth, the effectiveness of predictive technologies and other Big Data applications is based on specifically entering complex data in the system to develop algorithms to facilitate future operations. Complete data sets are rare, particularly in studies of terrorism, and even if such data is available, the scientists that enter it may fail to capture all the variables required for detailed projections. These errors may reduce the effectiveness of anti-terrorist activities or may be used for harassing innocent people.

Sixth, one must be aware of the imperfections of computer data analysis and always set the margin of error. The aggregated data may provide the information that it is highly probable that the given person will, in the future, join a terrorist organization. We would like such a person to be punished in advance for the act they have not yet committed. This would mean penalization for certain propensities we either are born with or acquire in our lifetime. Ronen Horowitz, former head of the IT unit of the Israel Security Agency, stated that predictive programs are applied, with high level of success, by the Israeli army and intelligence agencies to track enemies of the state.[28] The data that is used is in the form of videos, images, texts, and speeches. The projections that led to arrests may seem effective, because the number of terrorist incidents dropped sharply between 2015 and 2017, but it would take further analysis to specifically connect the arrests to a decrease in terrorist activities.

Seventh, the capacity of Big Data cannot be overestimated. As noted by Mark M. Lowenthal, some of the most difficult challenges of intelligence – such as recognition of the intentions of foreign leaders – will not be explained by Big Data because, simply enough, there is

[27] M. Maurtvedt, *The Chinese Social Credit System. Surveillance and Social Manipulation: A Solution to 'Moral Decay'?*, 2017, <https://www.duo.uio.no/bitstream/handle/10852/60829/Master-s-Thesis--Martin-Maurtvedt--27-11-2017.pdf>, 12 May 2019.

[28] B. Schaefer, "Predicting Terrorism: Implications for Big Data in Public Safety", *Georgetown Security Studies Review*, 8 April 2018, at <http://georgetownsecuritystudiesreview.org/2018/04/08/predicting-terrorism-implications-for-big-data-in-public-safety/>, 12 May 2019. A. Rapaport, '*Quite a few Terrorists lost their lives owing to Big Data*', 3 January 2015, at <https://www.israeldefense.co.il/en/content/quite-few-terrorists-lost-their-lives-owing-big-data>, 15 December 2020.

no sufficient data on that subject.[29] That is probably the case, but if the intelligence expectations are lower, such as associated with recognizing connections among leaders that had not been known before, the set objective may be achieved. Even if the context and causality of those relations remain unknown, different behaviors are correlated to currently known factors.[30] That is why the next challenge is going to be explaining *the analytical insights premised on big data to policymakers, who will hopefully ask responsible, hard questions, and be skeptical of taking action on the basis of foggy relationships. Thresholds and policies will need to be established regarding the taking of various operational, investigative, and policy steps in response to what will sometimes be uncertain correlations*.[31]

Despite the success of the predictive programs listed in the article, thus far no failsafe systems have been developed, because, in practice, the knowledge of where a crime may be committed does not always reduce violence in the given area. The evidence is visible in the results of a predictive policing program conducted by the Chicago police in 2016.[32] Even though they do not refer to combating terrorism, but rather crime, they illustrate the possible errors of data analysis. The study revealed that although it was possible to determine the place where a crime would be committed, the level of crime in Chicago has not been reduced significantly. The police did not know who would be attacked, so crimes were not prevented. In turn, it could be assumed that in the case of tracking terrorists, predictive analysis would be more effective, because a terrorist attack requires more long-term planning and secret organizational relationships. So far, however, these programs have not been unequivocally evaluated.

SUMMARY

At the end of the 18th century, Jeremy Bentham developed the Panopticon, a perfect prison based on permanent surveillance of prisoners who were not aware of being observed. It is possible that with modern IT technologies, ubiquitous video cameras, and fast analysis of big data sets, the reality of the 21st century is a manifestation of an idea from over two hundred years ago. The image of a society, in which everything is under control, is to provide not only the safety of citizens and state, but also to play disciplinary and preventive roles.

One might say that after the 9/11 attacks, the image of a controllable society has even become an obsession of the Western world. Civil rights and liberties are at stake because combating terrorism requires a more efficient intelligence system making use

[29] M.M. Lowenthal, "Intelligence Education: Quo Vadimus?", *American Intelligence Journal*, vol. 31, no. 2 (2013), pp. 7-11.

[30] M. Landon-Murray, "Big Data and Intelligence: Applications, Human Capital, and Education", *Journal of Strategic Security*, vol. 9, no. 2 (2016), pp. 92-121, at <https://scholarcommons.usf.edu/jss/vol9/iss2/6>, 20 May 2019.

[31] Ibid., p. 101.

[32] J. Saunders, "Pitfalls of Predictive Policing", *Rand Corporation*, 11 October 2016, at <https://www.rand.org/blog/2016/10/pitfalls-of-predictive-policing.html>, 4 June 2019.

of advanced IT technology to explore data. The concerns associated with using those tools, including loss of privacy, result in justified controversies and fear. However, it seems that, unfortunately, US president Barack Obama who noted that *you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience*.[33]

As demonstrated in this article, the technological progress of today has allowed security specialists to collect faster and process more effectively larger and more diverse data sets. The strengths of algorithm analysis listed above, as well as limitations of traditional intelligence methods, such as human intelligence (HUMINT), explain why Big Data tools are more and more important in the processes related to national security. Naturally, Big Data does not always operate better than people. As demonstrated by psychological research, in predictable situations algorithms are almost always better than human evaluation. However, in unpredictable situations resulting from sudden change, automated analysis may prove to be wrong.[34] In such situations, experts may rely on their intuition and vast analytical experience. In turn, algorithms may help in detecting the trends that are not obvious and impossible to note 'with the naked eye'. By combining information from different sources without any apparent significance, one may discover schemes and correlations that will allow better understanding of the studied phenomenon. That is why Big Data applications are best used when they allow people *to do what they do well – think, ask questions, and make judgments about complex situations*.[35]

Based on the Chinese experience, one may develop an even more effective system of analyzing aggregated data from different sources, which will be associated with practically a total loss of privacy. So far, the concerns associated with limitation of civil rights and liberties have restricted the inclinations of heads of state to develop a system of mass electronic surveillance. However, it seems possible to observe a general tendency of change in the approach of governments to citizens and, step by step (not suddenly and radically, like in the case of China), their rights are being limited. In turn, contemporary unconventional threats to security increase the temptation to develop reliable tools for data prediction and analysis. That is why development of a European or American Social Credit System may only be a matter of time. It is even possible, of which the author may not know, that such systems are already being tested.

BIBLIOGRAPHY

CONTEST The United Kingdom's Strategy for Countering Terrorism, June 2018, at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf>.

[33] M. Maurtvedt, *The Chinese…*

[34] D. Van Puyvelde, S. Coulthart, M. Shahriar Hossain, "Beyond the Buzzword…".

[35] Ibid.; "Enabling Distributed Security in Cyberspace. Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action", *Department of Homeland Security*, 23 March 2011, at <https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>, 1 June 2019.

Creemers R., "China's Social Credit System: An Evolving Practice of Control", 9 May 2018, *SSRN Electronic Journal*, at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792>.

Cukier K., Mayer-Schonberger V., *Big data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2014.

Dziwisz D., "Algorytmiczna przyszłość – ucieczka od wolności ku 'opcji domyślnej'", in P. Szymczyk, K. Maciąg (eds.), *Człowiek a technologia cyfrowa – przegląd aktualnych doniesień*, Lublin 2018.

"Enabling Distributed Security in Cyberspace. Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action", *Department of Homeland Security*, 23 March 2011, at <https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>.

"Global Terrorism Index 2017. Measuring and Understanding the Impact of Terrorism", *Institute for Economics and Peace*, at <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf>, 8 May 2019.

Home Secretary Announces New Counter-terrorism Strategy, 4 June 2018, at <https://www.gov.uk/government/speeches/home-secretary-announces-new-counter-terrorism-strategy>.

Inkster N., *China's Cyber Power*, London 2016, https://doi.org/10.4324/9780429031625.

Jussawalla M., Taylor R., *Information Technology Parks of the Asia Pacific: Lessons for the Regional Digital Divide*, London 2003.

Landon-Murray M., "Big Data and Intelligence: Applications, Human Capital, and Education", *Journal of Strategic Security*, vol. 9, no. 2 (2016), at <https://scholarcommons.usf.edu/jss/vol9/iss2/6>.

Larson C., "Twitter Data Mining Reveals the Origins of Support for Islamic State", *MIT Technology Review*, 23 March 2015, at <https://www.technologyreview.com/s/536061/twitter-data-mining-reveals-the-origins-of-support-for-islamic-state/>.

Larson C., "Who Needs Democracy When You Have Data?", *MIT Technology Review*, 20 August 2018, at <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>.

Lowenthal M.M., "Intelligence Education: Quo Vadimus?", *American Intelligence Journal*, vol. 31, no. 2 (2013).

Maurtvedt M., *The Chinese Social Credit System. Surveillance and Social Manipulation: A Solution to 'Moral Decay'?*, 2017, <https://www.duo.uio.no/bitstream/handle/10852/60829/Master-s-Thesis--Martin-Maurtvedt--27-11-2017.pdf>.

Peters G., "Counterterrorism: Trying to Predict the Future", *Army Technology*, 16 September 2015, at <https://www.army-technology.com/features/featurecounterterrorism-trying-to-predict-the-future-4654343/>.

Rapaport A., '*Quite a few Terrorists lost their lives owing to Big Data*', 3 January 2015, at <https://www.israeldefense.co.il/en/content/quite-few-terrorists-lost-their-lives-owing-big-data>.

Salm L., "70% of Employers are Snooping Candidates' Social Media Profiles", *CareerBuilder*, 15 June 2017, at <https://www.careerbuilder.com/advice/social-media-survey-2017>.

Saunders J., "Pitfalls of Predictive Policing", *Rand Corporation*, 11 October 2016, at <https://www.rand.org/blog/2016/10/pitfalls-of-predictive-policing.html>.

Schaefer B., "Predicting Terrorism: Implications for Big Data in Public Safety", *Georgetown Security Studies Review*, 8 April 2018, at <http://georgetownsecuritystudiesreview.org/2018/04/08/predicting-terrorism-implications-for-big-data-in-public-safety/>.

Treverton G.F., "New Tools for Collaboration. The Experience of the U.S. Intelligence Community", *CSIS*, January 2016, at <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160111_treverton_newtools_web.pdf>.

"Using Big Data Effectively in the Fight Against Terrorism", *Defence Contracts Online*, at <https://www.contracts.mod.uk/do-features-and-articles/using-big-data-effectively-in-the-fight-against-terrorism/>.

Van Puyvelde D., Coulthart S., Shahriar Hossain M., "Beyond the Buzzword: Big Data and National Security Decision-making", *International Affairs*, vol. 93, no. 6 (2017).

Zhou C., *Credit Information Database in China*, conference paper, Kuala Lumpur, 5-9 November 2012, at <https://www.ifc.org/wps/wcm/connect/e722b080438c5bc481f5b9869243d457/Session_8_C.Zhou_credit+database+in+China.pdf?MOD=AJPERES>.

Dominika DZIWISZ, PhD, is an assistant professor in the Institute of Political Science and International Relations of the Jagiellonian University in Krakow, Poland. She holds master's degree both in International Relations as well as Marketing and Management. She received her PhD with distinctions from the Jagiellonian University in 2014. Her PhD research was focused on cybersecurity policy in the USA. This topic, together with critical infrastructure protection and the relationship between Big Data and human rights, to this day remains in the center of her research interests.