10.53477/2284-9378-21-30

STRATCOM PREDICTIVE DATA ANALYSIS FOR STRATEGIC PLAN FORECASTING

Associate Professor Maria Magdalena POPESCU, PhD*

The idea of gathering intelligence from open source, human or social media as regular practice for structures in the field has been a frequently debated topic for specialized literature. Unlike this, gathering intelligence from corroborated Strategic Communication (StratCom) sources and instruments so that the information extracted that way be later on stored in databases and sieved through predictive analytics software to then reveal state or non-state actors' measures and behaviors has recently been shared as a novel thesis of the present author and recently taken over by doctoral schools in the field. The current paper provides an extended insight into the topic, to consolidate the construct.

Keywords: strategic communication; interoperability; predictive analytics; data; intelligence.

Motto: ”The essence of the independent mind lies not in what it thinks, but in how it thinks.”
Christopher Hitchens

Information abundance and data explosion, more and more acute polarization and the ever changing power status globally due to vanishing values, uncertainties connected to identity and status bring to the forefront more and more security of the individual and of the world. The technological progress that is more and more rapid triggers enhanced productivity in automation while artificial intelligence records and replicates human reactions, generating a war of influence and perception, with implicit impact on security, generating threats to democracy and to the state per se. Among the objectives that are under threat one finds social cohesion, one's identity simultaneously altered with psychological processes, the frailty of trust in authorities and the amplitude of disinformation, of propaganda with major effects on human behavior.[1] In this context, new media as well as a continuous development of the variety of instruments in social media, entertainment or information environments bring simplification but also a diversification of the interaction manners, ubiquity and responsivity they bring the virtual space in a tacit coexistence and complicity with individuals in a society, a replica of reality, close to a perfect copy. The attacks now develop through image, symbolic communication, common lexis and they target public perception but also the image of the actors that share the balance of power. Translating these interactions in the online environment generate the change in the way things are expressed, uttered, with success on the versatile and fluid receptors. State level and society level security is thus accomplished with new, interdisciplinary approaches from the intelligence services where the connection with individuals, with public institutions and with mass communication ones (mainstream media and new media) is based on a variety of products among which we mention the cultural ones, open sources (OSINT), human sources (HUMINT), the communication ones (COMINT), those connected to social media ones (SOCMINT), that bear, today, chameleonic shapes, adapted for the targeted threat, but all appealing to words, to perception and identity, to image. At the same time, automated character, information recurrence, sense permutation through user generated content, anonymity, impersonal character and meaning distortion up to a totally different representation, augmentation of hostile uses and of phishing attacks, transforming products into manipulation instruments through generating disinformation content for any of the media, mainstream or new media, for the social media as well, *deepfake* and *fake news,* disseminate narratives that influence governments, individuals , placing those involved

***”Carol I” National Defence University**
e-mail: *popescu.maria@myunap.net*

in communication on different levels of power.

The pandemic and the related *infodemy* demonstrate that wars of the world can now be led without conventional ammunition, just based on the power of word and perception, wakening individuals’ trust in state institutions, which leads to weakening internal and national security. At the same time, a lack of training in managing, decoding and management of information at society, nation and state level augments vulnerability in front of all these attacks.

In this context, security of a state and security at international level within the current coordinates, can be recovered and maintained through a constant knowledge of the evolution in communication means, in ways of expression that become more and more versatile, in senders and receivers that are ever changing and generate more and more changing broadcasting environments. Uncertainties that come from permanent changes find answers at *interoperable* level, through accessing the extended knowledge pool and common capabilities, through correlating instruments and messages that generate narratives, saving collected data and placing them, afterwards, in a *probabilistic analysis* process that can generate models of action and behavior to anticipate and counteract some unwanted dynamics.

Extracting data that would later undergo specific analysis is a process that is most wanted to areas fed with strategic messages, areas that engage global community: public relations, journalism, propaganda, public and cultural diplomacy and all that is an endeavor for defining a country’s image by promoting certain models in an attempt to redefine as many perceptions as possible to aid own interests, to meet very clearly defined objectives internally and internationally[2], according to NATO military concept for *Strategic Communication (StratCom):*

In NATO, *strategic communication* entails narrative strategies that bear messages destined to internal and external publics, while in the European Union, the strategic communication department focuses on public diplomacy for actions oriented mainly to promote values and policies of the union but also to counteract information threats that come from the eastern neighbors. The process of counteracting disinformation (…) includes detection and debunking, combatting and raised awareness of the instruments that support this phenomenon, which leads to a better social resilience, customized for the new types of threats and for raising trust in state institutions. Nationally, the 2020-2024 Country Defence Strategy highlights the importance of identification strategic narratives and underlines the development of digital competences for individuals in society, along with a training of critical thinking skills to lower the percentage of vulnerability in front of hostile messages produced by state and non-state actors equally, since ensuring a new security involves its diplomatic approach, the intelligence and counterintelligence ones, along with educational, health, cultural, demographic, economic, cybernetic ones, mainly all that defines life and safety of an individual at any level, through *soft power.* All these components, placed in cross-functional relationships, can augment resilience in front of the multifaceted, plurivalent and polyphonic threats, which are syntactically interoperable, only by a cross referential action, by transforming culture, values, education and language elements in a predictive modeling, to be organized in data pipelines, subdued to a probabilistic analysis, to generate models that contribute to understanding foreign actors’ strategic plans and consequently to building counteracting patterns for unwanted effects.

In this sense, strategic communication instruments’ syntactic and semantic interoperability facilitate intelligence gathering based on media, culture, diplomatic, economic and social representations that build the narrative arcade in security plans, therefore debunking discrete means of expression of the narrative structures which great powers issue can, through a form and content coordination and through feeding data pools especially built for this goal, to render with predictive analytics, the general image of strategic plans which great powers use internationally, fact that brings awareness and raising resilience as well as forecasting a neutralizing reaction in due time.

Syntactic and semantic interoperability in generating models of action

Generically, interoperability has been defined as the ability of two or more systems or components to exchange information for the benefit of using it[3]. Initially, interoperability has been seen in its technical understanding, with appeal to numerous hardware, software and data base systems. Open sources like Wikipedia or Google provide good examples for interoperability, through the systems' or software's capacity to exchange information and through the capacity groups have to cooperate, through the interaction and information exchange among automated systems, artificial intelligence and human operators, considering both friendly and hostile approaches. Once this concept has been transferred from IT area to communication processes supported by the communications systems, there is a transfer between system interoperability (interactions between hardware and operating systems) and the structural one (interactions between data models, data structures and schemata) on the one hand, to the syntactic one (the forms of the messages, their representations) and semantics (meanings provided by decoding messages). Syntactic interoperability allows information and intelligence in general to be properly used and disseminated while semantic interoperability allows the meaning of communication and metadata to be properly understood[4]. In other words, semantic interoperability is the capacity various agents, services and instruments have to communicate through information transfer, exchange, dissemination, while the genuine information, the basic one maintains its core.[5] Interoperability improves the process of sharing information, enhances awareness for each situation and facilitates the decision making process, as a benchmark element in problem analysis within any organization. Interoperability seen at this level is communicating with others, relying heavily on information digitization and on an identity that can be held responsible for any assumed status in various contexts.

In its turn, *interoperability* seen from a strategic perspective is activated through political, social, military, organizational factors and allows, through trans-disciplinarity, cooperation of all entities with common goal in solving each type of disequilibrium[6]. On the one hand, *syntactic interoperability,* found at the level of forms which the content gets, is accomplished once the systems found in this relationship use a communication and dissemination protocol, while on the other hand, *semantic interoperability* – found at content level, at the level of messages that have to be shared, is reflected in a simultaneous broadcast of meaning and its application in contingent reality. In other words, syntactic interoperability gathers various capabilities in the same pool while semantic interoperability connects these ones generating effects on the intended targets.

From this angle, *interoperability* becomes a solution for the new, unconventional, asymmetric, informational threats, when it is activated through *strategic communication (StratCom*) discourse and narratives, seen at political, military, economic, social and cultural level, to act through word and image, the new weapons of digital era conflicts. This is active and effective at the level of correlating strategic messages sent through the needed narratives on various dissemination channels, of intersecting diplomatic and strategic relationships internationally, through mainstream media and social media, both for positive narratives, that appeal and support, with content that are issued through public and cultural diplomacy, through *soft, smart* and *sharp power,* and for the negative, hostile narratives.

Connected to those previously presented, the diagram in *Figure 1* displays the relationship developed between *StratCom* instruments and its subcomponents. Semantic interoperability manifested at the level of this network provides synergetic content through key words and images that are recurrent thematically, while syntactic interoperability, highlights, through forms, the connections between the types of StratCom actions and representations that are compatible with media and social media, with cultural, artistic and educational products. To exemplify, a

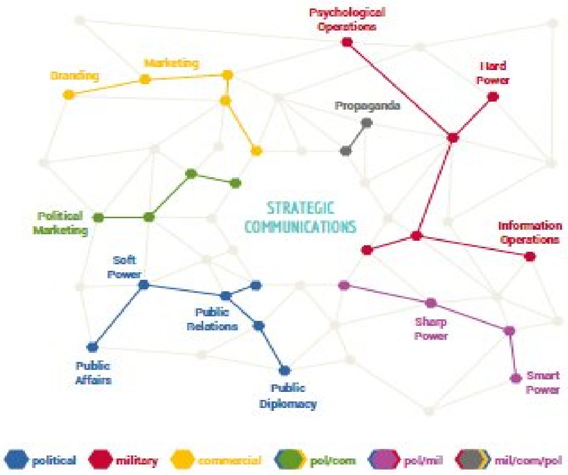

Figure 1 *Universul comunicării strategice (StratCom)*
Sursa: L. Haiden, 2017.

data base made with information extracted from correlating narratives disseminated via public relations, *smart power,* cultural, entertainment and educational products, public diplomacy and international relations measures will reveal, after predictive analytics, the strategic intentions on the international actors’ map. These intentions can be constructed from recurring key words or messages, from a sentiment analysis based on communities’ behavior and reactions within social media, all related to an analysis of the targeted public’s geolocation, considering the targeted field in the strategic narratives, shared as a result of economic or social impact measures, through cultural or educational exchanges, through support measures for carefully determined goals. With this data one can anticipate, in a probabilistic manner, models of action useful in counteracting hostile plans or in tailoring diplomatic decisions. Thus, strategic or operational plans can be forecasted for state or non-state actors. With *data-mining* and later on with data analysis one can show the most frequent dissemination channels, the most used apps for this, the sharing pattern for the targeted publics and the effects produced over society. Based on this analysis, used cultural stereotypes can be underlined along with the operating values. All can help configure the map of risks, vulnerabilities and security threats at state, organization and individual level.

Data predictive analysis based on strategic intelligence pools’ sources

In a generic approach we can state that strategic communication instruments, as they are represented graphically in Figure 1, placed in an interoperability relationship, represent an analysis lab for OSINT *(open source),* HUMINT (*human intelligence)* and SOCMINT (*social media intelligence),* once they become interoperable. After extracting data, *predictive analysis* is applied. The method is already applied in gathering intelligence that is to become, through data pools, subject to artificial intelligence software for the probabilistic analysis that generates models to counteract terrorism, a method effective in understanding the modus operandi of hostile actors, an effective instrument to locate threats in due time[7]. On the other hand, conceptually defined, *predictive analysis* involves *predictive modeling* which covers issues connected to the actors of the event, to its moment and to the reason of the performed endeavor, in other words- a concentration on the questions who? when? and why? connected to the individuals’ behavior pattern, involving the phenomenon of *forecasting* that is responsible for the potential of the behavior pattern in the future. It is through predictive analytics that one shapes models on non- processed data, coordinated with the already recorded ones for the topic history and extracted through processing the previous events, with a view to generate forecasts of potential risks. Literature in the field explains the event processing and identification of relevant elements through continuous monitoring, as well as through coordination with other elements, already registered in previous monitoring, from social media, from mainstream media, from organizations, manifestations, cultural and educational products, all placed in geospatial coordinates to trace the dynamics of the action, based on the structure or on the semantic messages already projected[8]. After data has been collected, trends, patterns and relationships among selected components are identified, characterized and modeled. Concrete uses of these methods and techniques have already been applied on sets of Twitter, messages, with a view to developing a model of crime and its frequency in a given timeframe, on a certain geographical area.[9] The correlations have evidenced possible connections[10] and have shaped common characteristics by resorting to key words that have generated the forecasting of similar events in the future based on recurrence and probabilistic methods. Same method has proved efficient in election sessions, financial markets events or natural disasters ones,[11] being in a direct proportion ratio with the data gathered – the more collected data and the bigger the intelligence pool, the higher is the probability to generate predictive patterns of potential risks.

Practical evidence of collecting and correlating data – China and StratCom actions

For a practical use of the theoretical aspects already presented, we shall display features from the current situation internationally, in pre- and post- pandemic coordinates. Considering the fact that individuals’ confidence has greatly lowered with respect to the political representatives, to media, participatory political attitude and religion, and based on the controversial and contradictory information wave on current problems on health, economy, individual's and nation's safety, one can understand the attitude members of the society have to look for alternative sources of information and thus to unwillingly become subject to disinformation, considering valid all the rumors and non-scientific sources, as well as the measures some states (like China, for example) take to penetrate the public space of the targeted society (information in social media about COVID-19, alternative therapies to fight the virus as well as different explanations for the origin of the virus) On the other hand, beyond the information trend that analysts have been focusing on, there are silent signals coming from many other instruments that communicate, in their turn, intentions reaching out from actors with certain interests in foreign publics.

The analysis of information flow or the one of the narratives war that tend to kneel down societies at large, one by one, call attention to more and more surprising strategies of those responsible for these things. Analysts have recently stated that Russia and China may cooperate in an exchange of experience- Chinese learn all that is connected to *trolls* while the Russians take up elements of Chinese *public diplomacy,* to recover Russia's foreign policy image. Moreover, in the same context, China is fighting a digital battle that is extremely difficult to confirm, based on influencing the perceptions of the neighboring countries' citizens, with lessons learned from the social media Russian trolls campaigns, a fight based on psychological operations, media and law operations to influence public opinion internally and externally, a fight that has been identified as more cunning than the Russian one, as stated by specialists, with an invasive diplomacy, that is totally different from the one used so far.[12]

Analyses published in the press[13] show that the pandemic has been the great opportunity for China to show the world that nothing can defeat an autocratic, solid and strong system, fact that has been proven through an intensified activity in the digital area, measured in an average of 300% raise on customized Twitter accounts aimed at foreign embassies, consulates, diplomatic personnel and public diplomacy related individuals meant to appeal through economy, infrastructure and all triggering the emotional side types of projects for the public at large.

What is interesting to be noticed is the multi-directional approach China has been using, and this may be considered as an integrating exercise for all those previously expressed in this paper so far.

On the one hand, if we speak about cultural diplomacy, one can see messages that China is trying to send to the world through video games, just like other countries, in strategically planned contexts. There are, for example, games whose topic of interest is a setting for cultural products output that advance beliefs, customs and ceremonies. Such a game can be considered *China Quest Adventure* which, based on Chinese history narratives, advances information on Chinese cultural values, through interactive collaboration-clothing, figureheads, weaponry, usual and daily expressions and topical vocabulary that urges, through key words, to approach the roles of the characters presented in the story and thus internalize each role's features, during the flow in the game. *Heart of China* and *The China Game* are other examples of games advanced and played in the international arena to promote cultural values. General cultural knowledge games make the gamers reach documentation and seek for knowledge before being able to answer and proceed to the next step, which is a proactive manner to share the intended information to the targeted audience.

To continue, any search engine access returns approximately two hundred video games whose action context is China, many of them produced by companies outside this country. Their topics are mainly kinetic, offensive and highlight the importance of gamer's decision, training the individuals for a mindset planned to win. Apart from promoting history, cultural values and important events, video games are designed as soft power diplomacy instruments, to appeal to support and sympathy from the intended audience in future projects.

As kinetic measures that accompany the non-kinetic cultural diplomacy measures, China has been manifesting itself since 2013, with the commercial plan to extend the historical *Silk Road* through the infrastructure projects *Belt and Road Initiative (BRI)* or *One Belt One Road (OBOR),* a measure that is relatively mild and open and which does not impose strict measures, allowing enough freedom to move for the political plans, an extension of soft power which tries to connect Asia to Africa, Russia and Europe, through a network of terrestrial infrastructure, while connecting the coastal area of China to South Pacific, Middle East and east of Africa, all the way to Europe, on a maritime route. Both strategies are meant to encourage the development of economic relationships. In this sense, a document issued by the European Bank for Reconstruction and Development[14] stated that the priorities these strategies aim at count, among others, on free trade, financial integrity, quality investment, social connection, goals that are effective in all the 14o states that have signed the memorandum of cooperation with China in this respect. The opening of a *Bank of China* branch in Bucharest confirms once again China’s interest for the projects related to economy and infrastructure in public-private partnerships. Together with this commercial plan, China manifests a silent innuendo, trying to develop its projects on infrastructure, investing in economy and promoting its values.

Through student exchanges, Chinese language courses and medical prevention programs, through fund donations meant to help research and through opening new Confucius Institutes coordinated by the ministry of education to run culture and language programs, China advances silently and tries to win as many segments of population from the targeted audience. Diplomatically speaking- while a cohort of analysts focused their attention towards Russia and its soft and smart moves, China is meticulously following its plans. Another example in this respect is the promotion of 5G implementation process, an extremely vocal step shaped in all kinds of advertising products until last April, which was re-initiated once the advertising campaigns were fueled again. In Romania Huawei was extremely aggressive in the pro-5G campaign: advertising videos, flyers and banners, online press conference, all these while China embassy was lobbying to the Romanian society for the need of an own, independent Romanian specific 5G network. However, not all the measures can be put into practice, and this was one of them, similar to the trial of investing eight billion euro in Cernavodă Nuclear Plant that ended in a complete failure in July 2020. Conversely, one cannot ignore that Lenovo has the highest computer trade market quota while Huawei comes in second for the smartphone trade market. This status is strengthened by cultural institutes, as mentioned before (Romanian Cultural Institute, in Beijing, Nicolae Milescu Chinese Cultural Center in Iași), the four Confucius Institutes and the video conferences organized by China, during the pandemic, to share information useful in prevention and control of the pandemic as well as in providing medical supply support.

We have presented here a new approach for smart power, that involves the strategic use of diplomacy through soft power, along with persuasion, with a development of new capabilities and with a projection of power and influence through alliances and partnerships, with or without military involvement.

In the context of these multi-directional evolutions, with versatile and covered attack coming from more adversaries, sharper analyses are mandatory, aided by a strategic intelligence gathering corroborated with the international politics’ interests and events and with measures to counteract based on specifically tailored anti-narratives.

Syntactically, the forms that carry all the kinetic and non-kinetic plans hostile actors generate and semantically, the meanings that any of these plans can share and send, need to be synergetic, they need to be congruent to generate data for analysis and to thus be able to debunk the meanings intended through each and every action, if danger is imminent, because semantics restricts meaning to action.[15] We thus use language to generate action and that is why a discrete analysis of the meanings each event or word bears, generates major implications in intelligence, security and defence, depending on the context in which the meaning was sent and on the representation it had on the outside. Graphically represented, syntactic and semantic interoperability through strategic communication instruments can be presented as seen in Figure 2.

That is why, intelligence gathered from digital sources, be they 2D or human, sending messages shaped in various forms, all bearing narratives generated by state or non-state actors, can help in building counter narratives, in a post analysis stage. Once the source, content, circumstances and the impact are evaluated, counter-narratives can be generated based on the forecasting issued

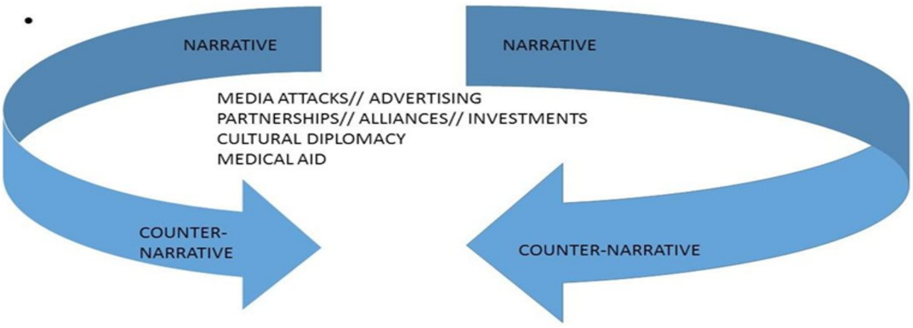

Figure 2 *Syntactic and Semantic Interoperability graphic presentation* (author's view)

subsequently. This method is already in use in DebunkEU.org.

Conclusions

The central element of those presented so far is the interpretation of information collected from the contingent reality to uncover deep structures that lead to the accomplishment of the communication goal. Intelligence analysis is based on interpretation, intertextuality, to penetrate the discrete structures of the communication products, to understand persuasion or its lack among the targeted audience. Thus, analysis of discourse, of images, of cultural products – films, music, of the educational ones-courses and their lessons can highlight what cannot be seen with a naked eye – i.e. the way symbols serve as means to generate meaning and the way power can be seized through daily conversations and interactions. Discourse and its narrative are constitutive elements that debunk the game between information and power and it is the first mechanism that creates knowledge, built on language, which gives meaning to things and social practices. The critical analysis presented in this paper states the importance of stressing on the linguistic mechanisms and their importance for strategic communication in a state security, since linguistic mechanisms allow individuals to be friendly or hostile and convince any audience about building a reality congruent to their interests, subduing others by using symbols, by persuasion.[16]

NOTES:

1 I. Chifu, „O periodizare a amenințărilor globale. Cea de a cincea generație de amenințări”, *Infosfera*, 4/2019, pp. 3-17.

2 A.S. Tatham, Strategic Communication: A Primer, vol. 8-28 of special series, Defence Academy of the United Kingdom, Advaced Research and Assessment Group, UK, 2008.

3 Marcia Lei Zeng, ”Interoperability”, Knowledge Organization 46, no. 2, 2019, pp. 122-146.

4 T. Koch, ”Establishing rigour in qualitative research: the decision trail”, Journal of Advanced Nursing, 53, 2006, pp. 91-100.

5 ML Zeng & LM Chan, Encyclopedia of Library and Information Sciences, 4th edition, 2015, pp. 4645-4662.

6 T. Slater, ”What is Interoperability?”, Network Centric Operations Industry Consortium - NCOIC, 2012, https://www.ncoic.org/what-is-interoperability/, accesat la 30.08.2020.

7 B. Lozada, ”The Emerging Technology of Predictive Analytics: Implications for Homeland Security”, Information Security Journal: A Global Perspective, 23:3, 2014, pp. 118-122.

8 Y. Zhu, L. Fei, N. Yang, ”Trustworthy software development based on model driven architecture”, apud Yang Y, Ma M, Liu B. (eds) Information Computing and Applications. Communications in Computer and Information Science, vol. 391, Springer, Berlin, 2013, pp. 193-202.

9 C. McCue, ”Data Mining and Predictive Analytics in Public Safety and Security”, IT Professional, vol. 8, no. 4, 2006, pp. 12-18.

10 MS Gerber, 2014. Predicting Crime Using Twitter and Kernel Density Estimation. Decision Support Systems, Volume 61, 2014, pp. 115-125.

11 E. Kalampokis & E. Tambouris & K. Tarabanis, ”Understanding the Predictive Power of Social Media”, Internet Research, vol. 23, no. 5, 2013, pp. 3-31.

12 U. Čereknova Bērziņa, The People's Republic of China and the Russian Federation as Strategic Allies, Riga: NATO Strategic Communications Centre of Excellence, 2020.

13 https://romania.europalibera.org/a/demascarea-chinei-cum-a-profitat-beijingul-de-povestea-covid-19/31254371.html- accessed on 20.05.2021.

14 https://www.ebrd.com/what-we-do/belt-and-road/overview.html-accessed on 22.05.2021.

15 JL Austin, How to do things with words, Clarendon Press, U of Michigan, 1962, p. 134.

16 Hartnett S.J. & Stengrim L.A., Globalization and empire: The US invasion of Iraq, free markets, and the twilight of democracy, Tuscaloosa: University of Alabama Press, 2006, pp. 417-441.

REFERENCES

Austin JL, *How to do things with words*, Clarendon Press, U of Michigan, 1962.

Čereknova Bērziņa U., *The People's Republic of China and the Russian Federation as Strategic Allies*, Riga: NATO Strategic Communications Centre of Excellence, 2020.

Chifu I., „O periodizare a ameninţărilor globale. Cea de a cincea generaţie de ameninţări”, *Infosfera*, 4/2019.

Gerber MS, *Predicting Crime Using Twitter and Kernel Density Estimation. Decision Support Systems*, Volume 61, 2014.

Hartnett S.J. & Stengrim L.A., *Globalization and empire: The U.S. invasion of Iraq, free markets, and the twilight of democracy*, Tuscaloosa: University of Alabama Press, 2006.

Kalampokis E. & Tambouris E. & Tarabanis K., ”Understanding the Predictive Power of Social Media*”, Internet Research*, vol. 23, no. 5, 2013.

Koch T., ”Establishing rigour în qualitative research: the decision trail”, *Journal of Advanced Nursing*, 53, 2006.

Lozada B., ”The Emerging Technology of Predictive Analytics: Implications for Homeland Security”, *Information Security Journal: A Global Perspective*, 23:3, 2014.

McCue C., ”Data Mining and Predictive Analytics în Public Safety and Security”, *IT Professional*, vol. 8, no. 4, 2006.

Slater T, ”What is Interoperability?”, *Network Centric Operations Industry Consortium - NCOIC*, 2012, https://www.ncoic.org/what-is-interoperability/.

Tatham A.S., *Strategic Communication: A Primer*, vol. 8-28 of special series, Defence Academy of the United Kingdom, Advaced Research and Assessment Group, UK, 2008.

Zeng Marcia Lei, ”Interoperability”, *Knowledge Organization* 46, no. 2, 2019.

Zeng ML & Chan LM, *Encyclopedia of Library and Information Sciences*, 4th edition, 2015.

Yang Y, Ma M, Liu B (eds) *Information Computing and Applications. Communications în Computer and Information Science*, vol. 391. Springer, Berlin, 2013.

https://www.ebrd.com/what-we-do/belt-and-road/overview.html

https://romania.europalibera.org/a/demascarea-chinei-cum-a-profitat-beijingul-de-povestea-covid-19/31254371.html