The 18th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 9th-10th 2023

INTELLIGENCE IN THE ERA OF DATA AND EMERGING TECHNOLOGIES: IMPACT ON SECRECY, SOVEREIGNTY AND INFORMATION SHARING

PĂIUȘ Ioana Hermina

Doctoral School of International Relations and Security Studies, „Babeș Bolyai" University Cluj-Napoca, Romania

Abstract:

Intelligence plays a critical role in the functioning of governments, societies, and companies. It is the process of collecting, analyzing, and distributing information to inform decision - making. Historically, intelligence was generally kept unseen and undisclosed by nations and organizations. However, with the emergence of new technologies and their capacity to generate tremendous amounts of data, the nature of intelligence is swiftly evolving. This essay further investigates how this transformation is affecting secrecy, stability, and collaboration.

Secrecy has been a cornerstone of intelligence operations since their very beginning. It has been imperative to protect sensitive information and techniques from foreign adversaries and other potential risks. However, the development of new technologies is challenging this longstanding tradition. Above all, big data, AI, and machine learning are creating an abundance of accessible intel that is making it tough to keep intelligence activities fully concealed. For instance, social media platforms create massive amounts of data like personal info, location data, and connection networks - all of which can be used by intelligence agencies to detect threats and evaluate their behavior. On the other hand, the usage of this type of data for surveillance purposes has been heavily contested due to its intrusive nature and possible misuses of personal information.

Sovereignty and intelligence have a close relationship - states have typically defended their right to gather and examine data within their borders, without foreign interruptions. Today, however, new technologies are complicating this concept. Cyberattacks and cyber espionage can be conducted remotely, while the web's anonymity allows it hard to discern who is behind an offence. For that reason, nations are demanding more international regulations and standards concerning the use of technology in intelligence collection - rules designed to guard their autonomy.

Sharing of intelligence has long been an integral part of the information-gathering process, restricted to a few close entities. But with the help of modern technologies, such as cloud-based platforms, it is now possible to broaden this circle and share data in real-time. This evolution brings with it both advantages, such as increased collaboration, and risks like privacy and security issues as well as misuses of sensitive information.

To sum up, data and new tech advancements are transforming the nature of intelligence by presenting fresh obstacles as well as opportunities for governments, societies and agencies. Despite the convenience that these creations bring when collecting and analyzing data, there is still concern about privacy, security, and morality issues. For this reason, it is essential to fashion a complete system that properly weighs the advantages of modern technologies against the safeguarding of personal privacy, safety and human rights.

Key words: Intelligence; Secrecy; Sovereignty; Information; Emerging Technologies; Security.

1. Introduction

Intelligence plays a critical role in the functioning of governments, societies and companies. It is the process of gathering, analysing and distributing information to inform decision-making. In the past, intelligence information was generally kept hidden and undisclosed by states and organisations. However, with the advent of new technologies and their ability to generate huge amounts of data, the nature of intelligence is rapidly evolving.

This paper further investigates how this transformation affects secrecy, stability and collaboration. Secrecy has been a staple of intelligence operations since the beginning. It has been imperative to protect sensitive information and technologies from foreign adversaries and other potential risks. However, the development of new technologies puts this long-standing tradition at risk.

Sovereignty and intelligence have a close relationship - states have traditionally defended their right to collect and analyse data within their own borders without foreign interruption. Today, however, new technologies complicate this concept. Cyber-attacks and cyber-espionage can be carried out remotely, and anonymity on the internet makes it difficult to identify the perpetrator of a crime. For this reason, countries are demanding more international regulations and standards on the use of technology in intelligence gathering - rules designed to protect their autonomy. Intelligence sharing has always been an integral part of the intelligence gathering process, restricted to a limited number of close entities. However, technological developments have also raised challenges to maintaining secrecy. For example, the sheer volume of information available in the digital environment makes it difficult to keep intelligence activities completely hidden.

A significant change brought about by emerging technologies is the possibility to share intelligence information in real time. Cloud-based platforms and other technology solutions allow for wider intelligence sharing circles and closer collaboration between different entities. Increased efficiency, rapid information sharing and more effective identification of common threats could be an advantage.

Intelligence, historically, has generally been kept secret and undisclosed to nations and organisations. The advent of new technologies and their capabilities have generated huge amounts of data, with the nature of intelligence evolving rapidly.

Intelligence agencies have had to protect their covert operations, sensitive information and techniques from foreign adversaries and other potential risks. Big data, artificial intelligence and machine learning create an abundance of information accessible to all that makes it difficult to keep intelligence activities completely hidden.

New technological advances and data are transforming the nature of intelligence services, presenting new obstacles as well as opportunities for governments, companies and agencies. Despite the convenience these advances bring to data collection and analysis, there are concerns about privacy, security and morality issues.

The research methodology used in this study was based on an interdisciplinary approach, which involved a review of existing literature in the field of Intelligence, emerging technologies and their impact on secrecy, sovereignty and information sharing. The research also included analysis of relevant data and information available in public sources such as scientific articles, government reports and academic papers.

Contributions of this research:

- Analysis of the Impact of Emerging Technologies on Secrecy. This research has examined in detail how technologies such as big data, artificial intelligence and machine learning have altered the secrecy of intelligence operations. It highlighted how these technologies have generated huge amounts of accessible data, making it difficult to maintain secrecy in these activities.
- Impact on national sovereignty. The study examined how new technologies have challenged the concept of sovereignty in terms of data collection and analysis within national borders. It highlighted the need to develop international regulations to protect state autonomy in the face of cyber threats and cyber espionage.
- Information sharing and collaboration. The research highlighted how modern technologies, including cloud-based platforms, have facilitated the wider sharing of information between entities. The benefits of extended collaboration were discussed, as well as security and privacy risks.

2. What is intelligence in the age of data and emerging technologies?

Intelligence, in the age of data and emerging technologies, plays a critical role in the functioning of governments, societies and companies. In general, intelligence refers to the process of collecting, analysing and distributing information to decision makers. However, with the advent of new technologies and their ability to generate vast amounts of data, the nature of Intelligence is evolving.

New challenges such as Big Data, AI (artificial intelligence) and machine learning are creating a huge amount of available Intel that makes it difficult to keep intelligence activities completely hidden. It is essential to create a comprehensive system that weighs the benefits that new emerging technologies offer against ensuring privacy, security and human rights.

3. How does intelligence play out in the age of data and emerging technologies?

In the age of data and emerging technologies, intelligence manifests itself in a multitude of ways. The first major change is the enormous amount of data that can now be collected and analysed using new technologies such as big data, machine learning or AI. These tools enable fast and accurate analysis of large volumes of information.

Wang and Chen (2018), examine in their scientific paper entitled "Intelligence Analysis in the Big Data Era: From Data to Knowledge" the challenges and opportunities presented by the emergence of Big Data in intelligence analysis. The importance of transforming raw data into valuable knowledge can influence decision-making in Intelligence.

Leveraging emerging technologies and Big Data analytics can provide significant benefits in Intelligence. Continuous adaptation to technological changes and development of ethical and efficient approaches are needed to harness the full potential of available information in the era of Big Data and emerging technologies (Wang and Chen 2018).

Managing Intelligence in the Big Data era requires adaptability and innovative approaches. The use of emerging technologies and the development of robust security policies and practices are essential to meet the challenges and harness the potential of intelligence information in the current context (Biltgen & Christian, 2016).

Establishing data sovereignty is about more than ensuring privacy, it requires the availability of controllable means of sharing information with others. In the context of large applications, dynamic consent mechanisms play a key role in directing information flows according to the proposed normative benchmark. Suggesting legal and governance issues to implement data

sovereignty: exploring notions of data ownership, targeting data literacy in education, encouraging transparency about data processing activities, and introducing representative data agents to analyse data flows according to individual preferences (Patrick Hummel, 2018).

"Living off the grid" is looking more and more like a concept from a bygone era, rather than a feasible option in our hyper-connected society. IARPA, under the auspices of the Pentagon, is at the forefront of revolutionizing the way we track and analyze global human mobility with an innovative project called HAYSTAC.

This initiative leverages data from interconnected devices and smartcity sensors, identifying irregularities in movement patterns that could signify potential emergencies. The Pentagon, over the next four years, plans to initiate more HAYSTAC-like projects, deepening our understanding of human mobility and increasing our ability to predict emergencies.

While it is essential to sociogenise the field of intelligence to avoid the illusion that it is completely new, it is also important to note the related transformations in the eruption of the digital age and the ease of surveillance, which facilitates both the sharing of information and the explosion of secrets and their discovery through internet technologies, as well as the role of private company services.

The scale and scope of surveillance and the transnationalisation of intelligence services that we have witnessed in recent years requires a new investigation of contemporary global security practices, on the one hand, and a careful mapping of the categories of analysis themselves.

Sovereignty, secrecy, security communities, territory, border control, technology, information, have inevitably come to mean different things to different people. The field of shared intelligence is dependent in its expansion and reconfiguration towards less HUMINT and more SIGINT activities on "the emergence of a digital state rationale based on the possibility for the intelligence services of different countries to extend their crime prevention and prediction objectives to a global area, convincing their own politicians that the future of intelligence services is clear: it must include and expand the technologies for collecting human activities.

This growth and need to collect digital intelligence and data, once politically accepted, has in turn fuelled wider transnational collaboration between intelligence services and national security professionals and led from expanding the category of foreign intelligence to sharing data that may be of national interest. This has created a spiral effect on projecting national security "from the inside out" through a transnational alliance of intelligence and national security professionals and sensitive data, creating an "outside in" suspicion effect for all internet subjects destabilizing the protection of national citizens when communicating with foreigners (Didier Bigo, 2019).

The next decade of artificial intelligence research will most likely be driven by efforts to integrate existing knowledge, promote new ways of learning, and make systems more powerful, generalizable, and trustworthy.

Research on the development of the human-machine cluster will be at the forefront, as will improvements in hybrid AI techniques and methods. Mastering collaboration and teamwork between humans and artificial intelligence is fundamental to future applications of artificial intelligence. Researchers are addressing this challenge by studying issues related to delegation of authority, observability, predictability, directability and trust.

Gaining a better understanding of how humans will learn to work with AI will in the future inform the creation of effective training programmes. Advances in language understanding are being pursued to create systems that can summarize complex inputs and through which to create a human-like conversation, a critical component of the next generation team.

New learning methods enable greater efficiency in both learning and inference from data. This reduces reliance on large data sets and broadens the openness of systems to handle tasks beyond their original scope, building pathways to contextual learning and common sense reasoning.

Hybrid AI techniques combine different approaches to harness their complementary strengths. Compared to humans, even today's most powerful artificial intelligence lacks what might be called 'common sense reasoning'. Efforts are being made to create different systems that can generalise knowledge and transfer learning between domains.

Artificial intelligence systems equipped with common-sense reasoning could effectively shape human ability to make and exploit assumptions about physical properties, goals, intentions as well as human behaviour, providing the ability to characterise the likelihood of probable consequences of an action or interaction.

Following the lines of research described above, a future is emerging in which artificial intelligence will govern humanity in unprecedented ways, unlocking capabilities in science, education, space technology, healthcare, infrastructure, manufacturing, agriculture, entertainment and a myriad of other fields.

Advances in natural language understanding could enable real-time translation and perception of more obscure languages for which written and spoken instructional data is limited, communication across geographic and cultural barriers, enabling business, diplomacy and the free exchange of ideas.

4. Impact on secrecy, sovereignty and information sharing

Information sharing is one of the most widespread and least regulated surveillance activities in our modern world. It is facilitated by rapidly changing technology, which has enabled the collection, storage and transfer of huge amounts of data within and between countries. The impact of these developments on privacy is significant.

Snowden's revelations about the practices of the National Security Agency (NSA) as the leader of an alliance composed of various SIGINT-internet intelligence services, show us that information that has been intercepted in digital space on the location of individuals and things, the identification of these individuals by linking together various data belonging to different bureaucracies and private companies, as well as information on social networks, is being shared between different foreign countries and sometimes for very different purposes.

The notion of shared secret information, even if it seems a paradox, to understand the current stakes in a world where the argument of global insecurity pushes different services to transfer certain information to their "counterparts" in allied countries, and the impact of this trans-nationalization of "national" security when the digital world destabilizes the borders of states. The notion of shared secrecy in the field of information sharing through procedures whereby a specific product of a logic of doubt about marginal behaviours (as if they were a sign of guilt) produces a list of suspects, who have no right to know why and how they became suspects.

In this case, secrecy is not strictly the opposite of information sharing, but the result of the collaboration of bureaucracies that allow the restriction to a certain "circle" of people in authority to keep others in the dark about the criteria for this suspicion and the ways in which they are assessed and the techniques they use. This creates a problem in terms of the rule of law and democratic principles, and entails new discussions on the boundaries between secrecy, security, publicity and control (Didier Bigo, 2019).

Shared secrecy has thus reconfigured the domain of secret service practices far beyond their official designations and has increasingly included traditional bureaucracies working at the borders, as well as many private companies, including those that are not internet providers but simply taken

up in the unmediated securing of everyday life. While many researchers accept this increase in the scale of information sharing and secrecy between an impressive range of actors, they still disagree on the reasons for such an increase. Technology now enables revealing analyses of types and amounts of data that were previously considered meaningless or incoherent.

Agreements between countries to share information are usually confidential arrangements and are not subject to public disclosure. As surveillance is carried out by different state actors, so is the exchange of such information. For example, the RAMPART-A program, owned by the National Security Agency ("NSA"), run with foreign partners, aims to gain "access to high-capacity international fiber optic cables transiting major congestion points around the world" (NSA 2023).

A leaked NSA document indicates that RAMPART-A can intercept "over 3 terabits per second of data flowing globally and includes all communication technologies such as voice, fax, modem, email, internet chat, virtual private network (VPN), voice over IP and voice call recordings.

MUSCULAR was a program jointly operated by the UK Government Communications Headquarters ("GCHQ"), which intercepted and extracted data directly as it transited to and from Google and the private data centers of Google and Yahoo, which were located around the world. According to a leaked 2013 document, over a 30-day period, the NSA sent more than 181 million records - consisting of content and meta data - back to data repositories at its centers.

Intelligence services use a variety of methods to secretly communicate and share sensitive information. Some methods:

- The encryption method is a technique whereby only the authorized recipient can read and understand the message. In encrypted form, information is transmitted so that it is difficult to understand for those who do not have the appropriate decryption key.
- Secure communication channels: Intelligence services use specially protected communication channels to transmit sensitive information. These can be VPNs, secure satellite communication networks or encrypted ones.
- Steganography method: This method consists of hiding secret information inside other types of data, such as images or audio files. By subtly altering this data, secret information can be hidden in a way that is not obvious to outside observers.
- Offline communications are those methods of avoiding detection. Intelligence services may resort to offline communication methods. This involves exchanging information through letters or personal meetings, thus minimising the risk of electronic interception.
- Secure collaboration platforms: These platforms involve strong authentication, advanced encryption and strict access controls, ensuring that only authorised individuals can access and share information.

Special attention is paid to steganography. It refers to the science of 'invisible' communication. Unlike cryptography, where the aim is to protect communications from a spy, steganographic techniques strive to hide the very presence of the message itself from an observer. The general idea of hiding certain information in digital content has a broader class of applications beyond steganography, the techniques involved in such applications are collectively referred to as "information hiding".

For example, an image printed on a document might be annotated with metadata that could lead a user to its high-resolution version. In general, metadata provides additional information about an image. Although metadata can also be stored in the file header of a digital image, this approach has many limitations. Usually, when a file is converted to another format, the metadata is lost. Similarly, cropping or any other form of image manipulation destroys the metadata.

Finally, metadata can only be attached to an image as long as the image exists in digital form and is lost once the image is printed. Hiding the information allows the metadata to travel with the image, regardless of the file format and image state (digital or analogue).

A special case of information concealment is digital watermarking. The process of embedding information into digital multimedia materials, within multimedia content, so that the information can be subsequently extracted or detected for various purposes, including prevention and control of copying, is called digital watermarking. This has become an active and quite important research area, and the development and commercialization of watermarking techniques are considered essential for contributing to and addressing some of the challenges faced by the rapidly proliferating digital content industry. In watermarking applications, such as copyright protection and authentication, there is an active adversary who would attempt to remove, invalidate, or counterfeit watermarks (M. Kharrazi, 2004).

As the implementation of big data applications and artificial intelligence intensifies across various sectors, a concept gaining prominence in discussions of responsible governance is the notion of data sovereignty. Although not uniformly used throughout the academic literature, the concept pertains to issues of control over who can access and process data. Historically, sovereignty denotes claims to absolute power over a domain, such as a sovereign nation-state's power within its territory. Calls for data sovereignty transfer this imagery into the realm of data and ICT: data sovereigns are those in a position to articulate and enforce claims of power over their data.

Taking data sovereignty as a normative reference point is not the same as endorsing and demanding respect for any claim of power. Compatible with, and undoubtedly inherent in the concept of sovereignty, is a relational aspect: whether a claim to sovereign power is legitimate depends on its content and the relationship between the presumed sovereign and the recipients of its claim. If arbitrariness or unreasonable self-interest drives the claim, sovereignty morphs into despotism.

Negotiating data sovereignty and its scope is a discursive process to be undertaken in dialogue with others and with society. In light of this, two levels at which data sovereignty can be affected can be distinguished.

Firstly, the sovereignty of nation-states appears compromised by the challenges and perplexities associated with aligning the online world (or parts thereof) with national legislation. For instance, commentators fear that governments using cloud computing might store data outside their jurisdiction, risking compromising national sovereignty by relinquishing control over information. This is why some authors identify data sovereignty with the ability to geolocate data, to place it within the borders of a specific nation-state, and to resolve uncertainties regarding the laws that apply.

Secondly, individuals cease to be data sovereign if they are unable to articulate or enforce claims of power and/or if they are unaware of the flow of their personal information, the nature of the data generated about their lives, who can access it, how it is processed, and the mechanisms by which such processing feeds back into their decision-making processes.

In the context of big data and automation, the meaning of individual data points cannot be fully understood in isolation. Their informativeness depends on how they correlate with other data points and sets. Data is decontextualized and recontextualized more quickly, easily, and frequently than ever before.

One hallmark of big data tools is their quest to identify unforeseen correlations. The future use of data, willingly and knowingly shared by people, is inevitable. Data processing and market concentration trends in the data field open the door to cumulative technological power across data from various domains of everyday life.

As mentioned, nearly all aspects of our lives are digitized. The connections between datasets blur boundaries, and the sphere of personal secrecy shrinks. Granting consent for data processing gives individuals control over their data as well as protection against potential harm. Users should have the option to decide how their information is used

When the complete anticipation of what will be done with an individual's data is not possible, and there is a lack of transparency, it means that the obtained information can be combined to reveal much more than the individual knows. To what extent does consent regarding the terms and conditions of a social media provider justify including customer data in epidemiological analyses?

One proposal is to seek broad consent from individuals for a variety of research activities that remain unspecified at the time of sample donation. While some defend such models, others criticize them for sacrificing the requirement of informed consent, which is vital for exercising self-determination.

Another option is to seek consent on tiered levels that authorize the use of a sample for a series of broadly defined research domains. Unfortunately, in our context, the very notion of tiers is deflated given the cumulative effects just described. If data tiers merge and overlap sooner or later, there might be a mere window to suggest that individuals targeted by data might realistically consent only to certain levels of data processing (Matthias Braun, 2018).

The concept of data sovereignty encompasses individual rights to connect and share information with others. Therefore, it demands not only constraint but also controllable data flows. We have highlighted a range of measures in law and governance designed more broadly that can advance this process: notions of data ownership, which target data literacy in education, encouraging transparency regarding data processing activities, and introducing dynamic consent models, as well as representation and empowerment models, systems that channel data flows in accordance with individual preferences.

Harari (H.N. Yuval, 2015) argues that the fusion of ICT and biotechnology has already given us the ability to form a "hacker," and that one day, pervasive and invasive technology will make human beings easy targets for "hacks" that will limit their freedom, as well as establish and maintain new power structures. Harari's bold statement, articulated in a diagnostic and provocative manner, will be a significant concern in discourses on responsibility and responsible development of technological innovations for many years to come. Regarding the prognosis of Harari's vision, the normative reference point of data sovereignty could be a promising step towards navigating the responsible, future-oriented, and hopeful handling of information technology possibilities.

Conclusions

The final conclusion regarding Intelligence in the era of data and emerging technologies is that there are immense opportunities as well as significant challenges when it comes to secrecy, sovereignty, and information sharing. This new paradigm is crucial for dialogue and collaboration among political actors, researchers, and industries to develop the best policies and technological solutions. Ensuring sovereignty, protecting secrecy, and promoting responsible and equitable information sharing are imperative for building a society based on fundamental values such as security, democracy, and sustainable progress.

The research has highlighted the importance of adapting to the changes brought about by emerging technologies in the field of intelligence and the need to find balanced solutions to address these challenges.

In the era of data and emerging technologies, intelligence is undergoing a process of continuous transformation and adaptation. The immense opportunities and significant challenges in the field have led to rapid developments in technologies such as artificial intelligence, big data, data

analytics, and the Internet of Things (IoT). Protecting the secrecy of information is a central concern in this context. A major challenge for intelligence services is the use of artificial intelligence and emerging technologies, which can bring both benefits and risks in safeguarding information due to the massive amount of data generated and collected. It is essential to develop innovative and secure solutions for cybersecurity to protect our information and data. Through a balanced and strategic approach, these solutions will counter cyber threats and ensure the highest levels of confidentiality.

By strengthening their data storage and processing capabilities, a nation ensures its informational sovereignty. This provides authorities and individuals with control over information and security in the context of emerging technologies, which bring opportunities for data sharing and dependence on external providers. It is important for states to safeguard their digital autonomy by protecting data integrity.

Information sharing in today's world can significantly accelerate decision-making processes and improve collaboration between states and organizations. We will need to find a balance between these advantages and the protection of personal information by safeguarding individual rights and freedoms and truly benefiting from all the advantages that information sharing offers.

A strong partnership between political actors, research experts, and technology leaders is needed to address challenges and benefits effectively. We can create appropriate policies and technological solutions to protect secret information, ensure sovereignty, and promote responsible and equitable communication through dialogue and best practices.

In conclusion, intelligence in the era of data and emerging technologies represents both a challenge and an opportunity for intelligence services. By adapting to technological changes and developing appropriate solutions, we can continue to ensure the security, sovereignty, and responsible sharing of information in an increasingly complex and interconnected world.

References:

[1] Biltgen P. & Christian, J. T. (2016). *Managing Intelligence in the Era of Big Data: Review of emerging trends and challenges*, Journal of International Intelligence and Counterintelligence, Nr. 29, pag. 40-61.
[2] Bigo, Didier (2019*). Intelligence and National Security*, Routledge Taylor and Francis Group, Vol. 34, Nr. 3, pag. 379–394.
[3] Botos, Horia (2018). *Business Intelligence and Competitive Intelligence*, Revista Stiintifica Research and Science Today, Nr.2.
[4] Braun, Matthias & Hummel, Patrik (2018). *Sovereignity and Data Sharing*, ITU Journal: ICT Discoveries, Special Issue Nr. 2, pag. 23.
[5] Chen H. & Wang (2018). *Intelligence Analysis in the Big Data Era: From Data to Knowledge*, IEEE Intelligent Systems, Nr. 33, pag. 82-86.
[6] Harari, Yuval Noah (2015*). Homo Deus. Scurta istorie a viitorului*, Editura Polirom.
[7] Lute, J. & Lucas, G. R. Jr. (2020). *The Impact of Emerging Technologies on Intelligence: A New Landscape for 2020*, Journal of Intelligence Studies in Business, Nr. 10, pag. 24-33.
[8] Martau, Ciprian (2017). *Securitatea Informatiei in Competitive Intelligence prin Steganogafie*.
[9] Schmidt, Eric (2018). *Final Report*, National Security Commission on Artificial Intelligence.
[10] Steckman, L. & Bresnick A. (2017). *Intelligence and Cybersecurity in the Age of Big Data: Current Trends and Future Directions*, Intelligence and National Security, Nr. 32, pag. 366-383.
[11] U.S. Army training and doctrine command (2015). *The Future of Intelligence Analysis in an Information Age: A Conceptual Model.* pag. 525.

[12] https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN20669_ATP%202-33x4%20FINAL%20WEB_v2_fix.pdf
[13] file:///C:/Users/ioana/OneDrive/Desktop/CARTI/2035%20cia.pdf
[14] http://sharif.edu/~kharrazi/pubs/ims04.pd
[15] https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29_0.pdf
[16] https://www.iarpa.gov/research-programs/haystac
[17] https://studyabroadnations.com/ro/cursuri-online-gratuite-de-management-al-calit%C4%83%C8%9Bii-cu-certificate/
[18] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363080