Technological trends: a focus on citizen security

Tendencias tecnológicas: un enfoque en la seguridad ciudadana

Tendências tecnológicas: um foco na segurança do cidadão

Luis Adrian Lasso Cardona[1]

Received: September 2th, 2020
Accepted: November 4th, 2020
Available: January 11th, 2021

How to cite this article: L. A. Lasso Cardona, "Technological Trends: a Focus on Citizen Security," *Revista Ingeniería Solidaria*, vol. 17, no. 1, 2021,doi: https://doi.org/10.16925/2357-6014.2021.01.02

Research article. https://doi.org/10.16925/2357-6014.2021.01.02

[1] Universidad del Valle - sede Buga, Colombia. Facultad de Ingeniería. Semillero SIEL-Univalle Buga.
Email: luis.lasso@correounivalle.edu.co
Orcid: https://orcid.org/0000-0002-3354-1554

Abstract

Introduction: This bibliographic review is the product of research on new technological trends, focusing on citizen security, carried out at the SIEL research center of the Universidad del Valle-Buga headquarters, Colombia in 2019.

Problem: Investigate new technological trends aimed at the citizen security sector.

Objective: Identify new technological trends in the sector of citizen security, their application in the world and exhibit the current state in Colombia.

Methodology: Review of scientific articles with criteria such as "big data", "artificial intelligence", "machine learning" and related to "security", in databases such as Scopus, Web of Science, IEEE Explore, Elsevier and Computer Source, and official documentation on recognized government web pages and newspapers, all from the past 5 years.

Results: Since MinTIC was created in Colombia, in partnership with different government entities, society in general has benefited from projects in areas such as education, health, housing and security. During the modernization of control institutions in Colombia, it is evident that the security sector is one of the most advantageous.

Conclusion: In general terms, sectors such as technology and education are still lagging behind. As for the security sector, there is no doubt the effort and progress in research and development of new technologies present in the vast majority of government entities.

Originality: New technological trends are investigated from the point of view of citizen security in several applicable scenarios.

Limitations: The vast majority of the review focuses on aspects of citizen security with very little connection between the social and educational fields. In addition, the information available regarding the use of technologies such as Artificial Intelligence and Machine Learning in Colombia was quite limited, making it difficult to compare with other countries.

Keywords: Big Data, machine learning, cybersecurity, predictive surveillance, citizen security

Resumen

Introducción: El presente artículo de revisión bibliográfica es producto de la investigación sobre las nuevas tendencias tecnológicas. Se hace un enfoque en la seguridad ciudadana, llevada a cabo en el semillero de investigación SIEL, de la Universidad del Valle-sede Buga, Colombia en el año 2019.

Problema: Investigar cuáles son las nuevas tendencias tecnológicas dirigidas al sector de la seguridad ciudadana.

Objetivo: Identificar las nuevas tendencias tecnológicas en el sector de la seguridad ciudadana, su aplicación en el mundo y exponer el estado actual en Colombia.

Metodología: Revisión de artículos científicos con criterios como "big data", "artificial intelligence", "Machine learning" y relacionado con "security", en bases como Scopus, Web of Science, IEEE Explore, Elsevier y Computer Source, y documentación oficial en páginas gubernamentales y periódicos reconocidos, todo de los últimos 5 años.

Resultados: Desde que se creó MinTIC en Colombia, en alianza con diferentes entes gubernamentales la sociedad en general se ha beneficiado con proyectos en áreas como educación, salud, vivienda y seguridad. La modernización de las instituciones de control en Colombia es evidente siendo el sector seguridad uno de los más aventajados.

Conclusión: En términos generales, sectores como tecnología, y educación aún se encuentran rezagados. En cuanto al sector seguridad, es indudable el esfuerzo y avance en investigación y desarrollo de nuevas tecnologías presentes en la gran mayoría de los entes gubernamentales.

Originalidad: las nuevas tendencias tecnológicas sean investigado desde el punto de vista de la seguridad ciudadana en varios panoramas de aplicación.

Limitaciones: En su gran mayoría, la revisión se centra en aspectos de seguridad ciudadana relacionando muy poco el campo social y educativo. Además, la información a disposición en cuanto al uso de tecnologías como Inteligencia Artificial y Machine Learning en Colombia fue bastante limitada lo que dificulto la comparación con otros países.

Palabras clave: Big Data, aprendizaje automático, ciberseguridad, vigilancia predictiva, seguridad ciudadana

Resumo

Introdução: Este artigo de revisão bibliográfica é o produto de uma pesquisa sobre novas tendências tecnológicas, com foco na segurança do cidadão, realizada no centro de pesquisas SIEL da sede da Universidad del Valle-Buga, Colômbia, em 2019.

Problema: Investigue as novas tendências tecnológicas voltadas para o setor de segurança cidadã.

Objetivo: Identificar as novas tendências tecnológicas no setor de segurança cidadã, sua aplicação no mundo e expor o estado atual na Colômbia.

Metodologia: Revisão de artigos científicos com critérios como “big data”, “inteligência artificial”, “aprendizado de máquina” e relacionados à “segurança”, em bancos de dados como Scopus, Web of Science, IEEE Explore, Elsevier e Computer Source e documentação funcionário em páginas reconhecidas do governo e de jornais, tudo dos últimos 5 anos.

Resultados: Desde a criação do MinTIC na Colômbia, em parceria com diferentes entidades governamentais, a sociedade em geral se beneficiou de projetos em áreas como educação, saúde, habitação e segurança. A modernização das instituições de controle na Colômbia é evidente, sendo o setor de segurança um dos mais vantajosos.

Conclusão: Em termos gerais, setores como tecnologia e educação ainda estão atrasados. Quanto ao setor de segurança, não há dúvida do esforço e progresso na pesquisa e desenvolvimento de novas tecnologias presentes na grande maioria das entidades governamentais.

Originalidade: novas tendências tecnológicas são investigadas do ponto de vista da segurança do cidadão em vários cenários de aplicativos.

Limitações: A grande maioria da revisão se concentra em aspectos da segurança do cidadão com muito pouca conexão entre os campos social e educacional. Além disso, as informações disponíveis sobre o uso de tecnologias como Inteligência Artificial e Aprendizado de Máquina na Colômbia eram bastante limitadas, dificultando a comparação com outros países.

Palavras-chave: Big Data, aprendizado de máquina, segurança cibernética, vigilância preditiva, segurança do cidadão

1. Introduction

The growth of the data generated in society has forged the need to optimize storage giving rise to what we now call Big Data, which overcomes the deficiencies of traditional systems to capture and analyze large volumes of data [1], which include textual content (structured, semi-structured and unstructured), and multimedia content (videos, images, audio) that are generated and stored on a multiplicity of platforms [2]. Recently, the ubiquity of the Internet of Things (IoT) has increased data collection (including health care, social networks, smart cities, agriculture, finance, education and more) on a huge scale. Based on the information available in databases, powerful techniques and tools can be used today that develop the ability to identify relationships, test hypotheses and analyze large volumes of data to find patterns that identify particular situations of safety, health, education, and business, among others [3]. In this sense, Machine Learning has gained great popularity in recent years due to its multiple application possibilities in many fields, including cybersecurity [4].

In a stricter sense, Big Data processing allows us to build predictive models to infer new "facts" at different times, environments, regions and cultures [5]. For example, in 2016, Chicago recorded a record homicide rate that surpassed New York and Los Angeles together. For this reason, the Police implemented a Big Data system that aims to stop crimes at the "pre-crime" stage. The system extracts data from the police force registry and awards points to people with a history. The authorities visit those with the highest score to warn them that they are being monitored and offer help from social services [6].

Ensuring citizen security implies large economic investments that in many cases cannot be faced by countries with emerging economies, which represents a strategic disadvantage against the great commercial and military powers. According to a research report from the Global National Security and Public Security Market - 2019-2024, published by Homeland Security Research Corp. (HSRC), a firm specialized in the National Security and Public Security industry, that advises institutions such as the US Army and Navy, NATO and the European Union, as well as government agencies from Japan, Korea, Taiwan, Israel, Canada, the United Kingdom, Germany, Australia, Sweden, Finland and Singapore, says that the Public Security and National Security market will increase from $ 431 billion in 2018 to $ 606 billion dollars for 2024. It also states that during the 2019-2024 period the predominant security technologies will be: Artificial Intelligence (AI), Big Data and data analysis, intelligent sensors, cybersecurity and AI-based video analysis, and 5G, TETRA and

LTE emergency communication. It should be noted that, in the preparation of this report, the markets of 43 countries were analyzed, among which we can mention the United States (US), the United Kingdom, France, Russia, China, Germany, Mexico, Brazil, Argentina and Colombia [7].

The current article is a product of the research center of the Universidad del Valle-Buga headquarters, Colombia, which aimed to identify the most important technological trends that will be relevant in the areas of public safety, emphasizing Colombia and placing it in the current and future landscape regarding the implementation of laws and related technologies. The study was conducted through a documentary review of primary sources of the last 5 years, such as: scientific articles, government pages, institutions of national and international renown, recognized laws and newspapers, which demonstrate the current and future of the topics discussed. It begins with a brief description of Colombia's national digital security policy to understand the relationship between the different state institutions and their interference in the development of security laws and plans. Subsequently, at the discretion of the researcher, a detailed description of each of the most important technological trends related to the subject in question is made. Finally, the conclusions of the review are established, showing the most relevant results from the researcher's point of view.

2. National digital security policy of Colombia

On April 11, 2016, the National Government of Colombia approved document CONPES 3854 that establishes the guidelines of the National Digital Security Policy, seeking to modernize the country and its institutions to react in a timely manner to possible risks and threats against its infrastructure and the digital information of citizens [8]. This policy is based on five work areas [9]: (1) Establish a clear institutional framework around digital security, based on risk management, (2) Create the conditions for multiple stakeholders to manage the risk of digital security in their socio-economic activities and generate confidence in the use of the digital environment, (3) Strengthen the security of people and the State in the digital environment, (4) Strengthen national defense and sovereignty in the digital environment, and (5) Promote cooperation, collaboration and assistance in digital security, nationally and internationally. The main virtue of this policy is that it is a tool aimed at preventing and improving the coordination of entities such as: the Ministry of Information Technology and

Communications (MinTIC), the Ministry of Defense with its Joint Military Cybernetics Command (CCOC), the Colombian Cyber Emergency Response Group (colCERT) and the National Police with the Police Cyber Center.

Since the implementation of CONPES 3854, the country has made significant progress. In terms of collaboration, the country signed a memorandum with the Organization of American States (OAS) to develop a cyber excellence center in Bogotá to share information and good practices and strengthen cooperation with international entities. In addition, the Police Intelligence Directorate (DIPOL) of Colombia implemented a platform that has as its central core a computer network with the capacity to process more than four million data items in a few seconds, which is based on technological models used by EUROPOL, the US Department of Defense and the New York Police, among others. In the first phase of implementation, agreements were established with more than 95 public and private databases, allowing infinite possibilities for real-time information crossings [10].

A notable result of the implementation of the new digital security policy was the implementation of a unified command between the public force, the Prosecutor's Office, the Ministry of Interior and the electoral organization to neutralize any intention to alter the electoral process in the last elections [11].

3. Technological trends

3.1. Big Data

Big Data is the term for a collection of data sets so large and complex that it is difficult to process them using conventional data mining techniques and tools. Its objective is to extract useful information from a large data set and transform it into an understandable structure for later use [12].

Frequently the term Big Data is described by 5 characteristics: "volume", "velocity" and "variety", creating the 3V model [13], which then went on to include "veracity" and "value" giving rise to the 5V model, described below: (1) Volume refers to the large amount of data generated, (2) Velocity refers to the speed at which new data is generated, (3) Variety refers to the types of data that we can now use [14], (4) Veracity describes the integrity, accuracy and quality of the data and (5) Value describes the benefits obtained by transforming the data [15].

3.1.1. Security Applications

The potential of Big Data depends on the sectors where it is used. For example: (1) in call centers to improve customer satisfaction, (2) in commerce by using social networks to understand customer preferences, (3) in banks to detect fraud in transactions, (4) in the financial market to analyze and classify the risk assessment and (5) in information technology to improve security [16]. In relation to security, NASCIO, the main network and resource for US state directors of information, established the top ten priorities for 2019 with a view to improving police management, highlighting the following criteria: data governance, strategy and predictive analysis, and Big Data [17]. For Emcien Inc., leader in the development of applications for predictive analysis, there are 4 cases in which intelligence and law enforcement agencies take advantage of Big Data for crime prevention [18]: (1) Social network analysis, which determines the most active and influential people in a criminal network; From calls, posts on Facebook, Twitter or email, the actions of a criminal or terrorist network are recorded, and Big Data processes them to help investigators get a faster response. (2) Files of apparently unrelated cases; Currently, analysis technologies can link cases that do not have a common attribute, but that have a match for two or more relevant attributes. (3) Crime prediction modeling; The combination of various data sources, such as arrest records, crime scene reports and incident reports help to create a model to predict criminal behavior. (4) Network monitoring and cybersecurity; Botnets, backdoors, rootkits, Trojans and worms are the tools used by criminals to infiltrate confidential data collected by governments, and in this regard, the detection of anomalies in data is one of the main tasks that Big Data supports.

In the area of security Big Data is having a great impact on society. Such is the case of the city of Shenzhen in China, where the Police are using Big Data for video analysis, along with intelligent methods of criminal investigation to solve homicide cases and similar crimes. Currently, the city has about 1.3 million video surveillance cameras, and according to statistics approximately 60 percent of criminal cases are resolved with the help of video surveillance and data analysis [19]. In the US, the Department of National Security Science and Technology uses a free application called Citrus, to create trends and link disparate data to support criminal investigations related to human trafficking networks, mainly through reports collected from Customs and Border Patrol staff (CBP). The CBP reports summarize the details of the migration patterns of foreigners, as well as the issues and associated networks responsible for smuggling activities [20]. Another example is the Geofeedia software, which is an intelligence platform to access Twitter, Instagram and YouTube content published by users located in a specific area. This software analyzes the data in order to obtain patterns and anticipate the crime [21].

3.1.2. Legal Risks of Big Data

The application of Big Data technologies still presents legal gaps that hinder its implementation by organizations, as well as increase the uncertainty of users by ignoring the treatment given to their personal data. Its use is questioned by human rights organizations and NGOs, who see it as a tool that can violate the privacy of citizens and expand, in some cases, the risk of social and economic discrimination based on the results of algorithms implemented for data analysis. For example, in the United States, it was discovered that a system technology used to assess the future risk of recidivism among defendants discriminated against black people. Similarly, in the United Kingdom, it was found that an algorithm used to make custody decisions discriminated against people with lower incomes [22].

In this regard, the European Parliament resolution of March 14, 2017, on the implications of Big Data in fundamental rights: privacy, data protection, non-discrimination, security and law enforcement, urges the Commission, the States members and data protection authorities in the points: 20, 21 and 22 to define and adopt measures to minimize algorithmic bias and discrimination. At point 25, he urges all agents of the security forces and agencies that use data processing and analysis, that this collection should always be adequate, relevant and not excessive in relation to purpose. It also indicates that decisions based solely on automated processing, including profiling, that produce negative legal effects for the interested party or that significantly affect it, unless authorized by the State, are prohibited [23]. In Colombia, the Constitutional Court held that the possibility of processing sensitive data without the owner's authorization must "be contained in a law, be in accordance with the guarantees granted by habeas data, for example, in terms of purpose, and comply with the requirements of the principle of proportionality" [24].

3.2. Machine Learning

Machine Learning (ML) refers to any computer algorithm that learns to perform a task directly from examples, without a human being providing explicit instructions or rules on how to do it [25], and the application of techniques for automatic pattern detection in significant data thereby matching the programs with the ability to learn and adapt [26]. Currently, we are surrounded by machine learning based technology: search engines learn how to deliver better results, anti-spam software learns to filter our emails, and credit card transactions are protected by learning software to detect fraud [27].

While Big Data is responsible for storing and managing data, ML applies techniques such as Naive Bayes (NB), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN) to detect trends that allow predicting situations in fields such as finance, health, neuroscience, transportation, education and public safety, among others [28].

One of ML's techniques is reinforcement learning, inspired by behavioral psychology, which helps software agents take action in an environment. Some cases are: (1) systems that develop predictions about current and future traffic conditions providing users with routing options based on that information, (2) computer games and (3) learning environments where simulations of real-life traffic situations help in the development of skills, which has a wide application, for example, in training activities, reducing the probability of accidents [29].

3.2.1. Machine Learning Applications

In the security sector, ML has multiple applications. For example:

- The Maven Project, developed for the US Department of Defense, uses artificial vision, AI and ML algorithms to process the video captured by the cameras of unmanned aerial vehicles in order to identify hostile activity, and help human analysts make more efficient and timely decisions based on the data [30].
- Lethal Autonomous Weapons Systems (LAWS), a U.S. Army weapon system that requires a computer vision system and advanced ML algorithms to classify an object as hostile, make a decision, and guide a weapon toward the target. This capability allows the system to work where others would not be able to operate [31].
- The New York Police (NYPD) developed Patternizr, a decision support tool and a recommendation engine consisting of a set of ML models to make the search for criminal patterns more efficient and effective [32]. Patternizr was manually trained for 10 years. In the tests, it accurately recreated the old criminal patterns a third of the time and returned parts of the patterns

80% of the time. To reduce possible racial biases, Patternizr does not examine the race of crime suspects when looking for crime patterns [33].

3.3. Cybersecurity

Cybersecurity is the activity of defending the technological assets of the institutions against the attempts of an adversary to meddle and take control of those assets in some way. "Defense" can take many forms: respond directly to the attacks, preventively investigate trends to anticipate the actions of the attackers, or decide what actions to take when a vulnerability is still exploited [34]. According to the threat report published in February 2019 by Cisco, in 2018 the incidents related to the most common security attacks faced by organizations are: Botnets and RAT (58%), Crypto mining (30%), phishing (9 %), Trojans (2%) and Bank Trojans (1%) [35].

3.3.1. Cybercrime costs

Worldwide, the costs incurred due to attacks on computer systems and physical infrastructure are enormous. In 2015, the intrusion to Anthem Insurance Company exposed the data of 80 million consumers, while the intrusion to the social network Ashley Madison exposed the data of 37 million consumers. In 2016, a breach in the critical electrical infrastructure of Ukraine and Israel resulted in power outages that lasted several days. In 2017, ransomware, such as WannaCry and Petya, affected numerous companies worldwide [36]. In total, about 250,000 computers were blocked by cybercriminals who requested a payment between 300 and 600 dollars [37]. It is estimated that by 2019, cybercrime will cost approximately $ 600 billion a year, compared to $ 445 billion in 2014 [38]. In Colombia, according to the report "Costs of cybercrime in Colombia 2016-2017" published by the Police Cyber Center, the main modality that affects citizens and businesses are scams; the most representative being: (1) the "Letter from Nigeria" with economic losses between 142 and 4,286 dollars, (2) Smishing (SMS of false prize) between 15 and 200 dollars, (3) Request for information of cards (Vishing) between 142 and 7,000 dollars, (4) Phishing (impersonation of bank accounts, government pages) between 60 and 14,000 dollars, (5) BEC (impersonation of corporate mail) where it is estimated that for each case there is a loss of 100,000 dollars and (6) Ransomware where recovery of an infected computer is between 0.5 to 5 Bitcoins [39].

Likewise, information hijacking is one of the most common cyberattack techniques for companies in the country. For example; "Indurtex", a textile company, suffered an attack from Russia that affected the server through a virus that hijacked the information and for which the criminals demanded a payment in Bitcoins, and before the refusal of the payment, the information was eliminated. A similar case occurred with the company "Rico Pollo", where the computers were blocked with an extortive message that demanded a payment in cryptocurrencies. The payment was not made either, and 5 years' worth of data was lost and an expense of 3.500 dollars had to be made in new licenses [40].

3.3.2. Cybersecurity Reports

According to the study "Trends in cyber risk management and information security in Latin America and the Caribbean (AL&C) 2019" by Deloitte, in which 150 organizations from 12 countries and 7 sectors participated, 40% of the organizations had suffered a cybersecurity incident in the last 24 months, 70% of organizations say they are not sure of the effectiveness of their incident response process, only 3% perform simulations to assess their effective response capacity, 31 % of organizations perform threat intelligence and share information with other organizations, and almost 7 out of 10 organizations have implemented a cybersecurity awareness program [41]. In Latin America, 63% of organizations allocate between 1% and 5% of the information technology budget to the cybersecurity area, while, in Colombia, 50% allocate those amounts. Regarding the use of basic security monitoring tools, in Colombia the most used protection is traditional antivirus software with 40% use and in Latin America, the figure is around 43% [42].

On the other hand, Comparitech, a company specialized in technological services, analyzed device infections, attacks on financial systems and the legislation of 60 countries to determine how safe they are against cybercrime. According to the results, Algeria has the worst cybersecurity index, Japan the best and Colombia is ranked 39. It states that in Colombia 12.52% of mobile devices are infected with some type of malware, compared to Japan which is 1.34%. Regarding the qualification of the legislation, which measures how up to date it is to provide cybersecurity guarantees, the country's score was 4 out of 10, with no country scoring above 7. On "How prepared the country is to resist a cybersecurity attack", the score obtained was 0.56 out of 1 [43].

3.3.3. Defense against cybercrime

One of the most used resources in cybersecurity is the Intrusion Detection Systems (IDS). An IDS is a software or hardware system that identifies malicious actions in computer systems to allow system security to be maintained [44]. With the help of technologies such as ML, AI and Big Data, an IDS can detect malicious attacks automatically. These, collect and analyze network traffic, security records, audit data and information of the key points of a computer system, to verify if there are security violations in the system [45]. For example; In the case of cyber-attacks with the WannaCry ransomware that were registered in 2017, companies that had security systems equipped with ML and AI responded better to this threat because they identified the traffic pattern that generated the incident, compared to those that did not have this technology [46].

An important criterion that stands out in the previous reports is the collaboration that can be established between the different institutions and States in order to respond to threats that affect public and national security; although security cooperation is much more complex than any other type of cooperation as in many scenarios it implies relying on other States for national survival [47]. In terms of cybercrime, a large number of countries in the world feel the need to establish agreements and pass laws that allow for the exchange of information to improve national security. This is the case in Colombia, where the National Police has been linked to international organizations such as INTERPOL and AMERIPOL, as well as to the different expert groups (Focal Point) of the European Center against Cybercrime (EC3) since 2014. In addition, since 2015, Colombia belongs to the Joint Action Group on Cybercrime Action "J CAT" aimed at articulating joint actions against transnational cybercrime networks [48]. Also, in early 2019, Colombia and Chile signed a memorandum to promote cooperation in cyberspace, cybersecurity, cyber defense, cybercrime and cyberintelligence, through the exchange of good practices, development and implementation of national plans, response to incidents in cyberspace, legislative development, information exchange, human talent, education and training, national capacity development, among others [49].

On the other hand, the Colombian government, through law 1928 of 2018, approved the country's accession to the Budapest Convention, increasing international cooperation to prevent and confront any crime and strengthen national laws and regulations against cybercrime to all levels [50]. In this sense, the National Police, within the framework of the "Joint Action Day", participated in 10 initiatives to combat fraud at the main airports in Europe and America, impacting 834 reports associated with 691 people, at 230 airports in 60 countries. This activity was organized by the member countries of EUROPOL and AMERIPOL. 171 SIENA newsletters were also shared with EC3, making Colombia an important ally for the exchange of information with Europe on criminal investigation [51].

While it is true that there are technological tools that help protect against cyber-attacks, it should not be ignored that education is a fundamental weapon. In the United Kingdom, improving cybersecurity education and skills is one of the four main components of the national program to guarantee cyberspace, incorporating cybersecurity at all educational levels from the age of 11 and supporting undergraduate and graduate research in areas of cybersecurity. Likewise, the Tempus Project of the European Commission studied the approaches of formal and informal education in the teaching of cybersecurity in the universities of the US, Europe, Asia and Australia, and public education in awareness and information campaigns [52]. In Colombia, document CONPES 3854, literal E4.5, determines that the Ministry of National Defense will design specialized educational content, participate in simulation exercises and train the multiple stakeholders responsible for guaranteeing national defense in the digital environment [8]. On the other hand, in early 2019, the National Government and Cisco signed a memorandum of understanding on innovation, entrepreneurship and cybersecurity, to promote the country's digital transformation, modernization of government institutions, secure connectivity and the country's competitiveness. In addition, Cisco will expand the reach of Cisco Networking Academy, its leading social responsibility program in education, offering classes and content on cybersecurity and other areas, to nearly 10,000 citizens [53].

3.4. Predictive surveillance

The ability to predict the future location of critical crime points confers countless advantages to a police force, including improving public safety. Police forces have used mapping tools to visualize and interpret patterns of past crimes, applying a retrospective process. Predictive approaches, on the other hand, involve methods that predict the future distribution of crime risk based on well-established models and assumptions [54], and applying neurocriminology, a specific branch of neuroscience that studies interactions between the brain, genes, the environment and individual predispositions to antisocial trends [55].

Predictive surveillance is a research field whose main objective is to develop machines to predict crimes using ML algorithms and the increasing availability of data. The forecast models estimate a crime rate, taking into account past criminal history (times and locations) and special data such as census variables, liquor store locations and probation information [56].

3.4.1. Models

Several algorithmic methods have been developed with the objective of identifying critical crime points based on social variables related to crime. Some of these models are [57]: (1) Analysis of spatial points; Investigate the movement of crime by identifying changes in spatial patterns / distribution of crime, (2) Mining association rules; A tool for discovering associations between different crimes, (3) Similarity of graphics; Identification and description of crime patterns, and (4) Series finder (supervised learning to detect patterns); identification of patterns in home invasion crimes.

3.4.2. Application cases

In the US, more than 50 police departments use PredPol software, as well as some forces in the United Kingdom. The ML algorithm is fed with historical data such as; type, location and timing of the crime, which are combined with many other socio-economic data, which are then analyzed by the algorithm in an attempt to predict where and when specific crimes will occur in the next 12 hours. The predictions are shown on a map using color-coded boxes, each representing an area of 500 square feet (46 square meters). Red boxes are classified as "high risk" and officers are recommended to spend at least 10% of their time there [58].

For its part, IBM developed a platform that combines powerful analytical and cognitive capabilities with structured and unstructured data (official notes, social networks and videos) of crimes, for crime prevention and prediction. This solution provides agencies with the means to make better use of staff and schedule patrols, making citizens and the police safer [59]. Similarly, the Naples police are using a program they called 'X-law', which has a predictive approach and was tested in Naples and the provinces of Prato and Venice with good results. Its algorithm is based on the concept that criminals have a modus operandi that rarely changes. The system sends information every half hour announcing where a crime is most likely to occur in the next two hours. Thanks to these mathematical calculations, the police can be more effective and prevent crimes with greater precision. Normally, a control patrol in Prato covers an area of approximately 125 kilometers per day. With the use of this technology, it is reduced to 23 kilometers, saving significantly on administration costs [60].

In Latin America, the city of Montevideo was the first to use this type of software to predict armed robberies and pickpockets, since these crimes have a direct impact on security perceptions in the city. In Chile, a group of researchers from the Security

Analysis and Modeling Center (CEAMOS), sponsored by the Universidad de Chile, is developing software similar to PredPol, but designed specifically for criminal patterns in Latin America [61]. In Salvador, Guatemala and Honduras, the capacities of national institutions to record and process crime information are increasing. Fundamentally, the information is used to analyze the incidence of crime, complemented by surveys and studies on gangs, violence against women and people trafficking, to guide the policies of civil society security and justice institutions and organizations [62].

In Cali, Colombia, during the administration of Gustavo Guerrero, data was collected on where and when the homicides occurred, revealing that the majority of the homicides occurred on weekends, often related to alcohol consumption and committed by young people. Based on these results, restrictions were applied, and according to a study published in the American Journal of Epidemiology, during the time they were implemented, homicides decreased by 35 percent [61]. On the other hand, in Bogotá, a project will be carried out between the Office of Information Analysis of the Secretariat of Security, Coexistence and Justice, the Universidad Nacional and the Quantil company, to develop crime prediction models combining databases of entities such as the National Police, the Prosecutor's Office or 123, together with the Big Data analysis of other sources of information such as images of the city's cameras [63]. It is expected that these studies will serve as input for the development of intervention and prevention policies and strategies, which will help in the significant and permanent reduction of crimes of greater impact for citizens, such as: homicides, fights and robberies [64].

3.5. Mobile communications and air surveillance

The use of technologies that allow for real-time communication is one of the most important strategies to be taken into account by the control, military and police institutions in the context of security, which, when integrated with aerial surveillance (drones), they obtain a greater panorama of the area to be controlled, making their management more effective, assigning the required personnel to those areas of greatest conflict. Drones represent an important intelligence resource, and the associated costs, as well as eliminating the risk to a pilot's life, are some of its main advantages [65]. Currently, its main use is focused on the civil field, being a fundamental part of the implementation of smart cities.

The Colombian Police have made use of these two technologies, which implemented the APPOLO platform (Full Personal Authentication of Logical Origin) on mobile devices, which allows for the online authentication of the citizen through fingerprint verification using the database of the National Marital status Registry. Also, in 2018, the Tactical Communications, Command and Control System with 28 drones was launched, aimed at maintaining contact between patrols deployed in different areas and operations centers, with real-time transmission of voice, data, video and photography, integrated with different forces and relief agencies [66]. Also, in June 2019, the Bogota Police launched five "Matrice 210" drones with the aim of guaranteeing public safety at strategic points such as bike lanes, parks, Transmilenio stations, social mobilizations, football matches and concerts. These have a high-resolution camera with a range of 7 kilometers and thermal vision. They can operate at 3 thousand meters ASL, at a speed of 80 kilometers per hour, and flying time of more than 30 minutes [67].

On the other hand, there is a great concern in the State forces about the use of this type of tool since they are practically undetectable, easy to use, relatively cheap and do not expose the life of the staff. In the future, attacks on strategic objectives of great military value are expected to be carried out by a fleet of drones. This technology already exists and is available in the market. A demonstration of the synchronization of these devices was held at the Winter Olympics in Pyeongchang, when 1218 perfectly coordinated drones illuminated the opening ceremonies in 2018 [68].

But the air domain is not the exclusive task of airplanes, helicopters or drones, it is also necessary to look above the clouds. Within the Colombian Air Force (FAC) since 2013, the Department of Space Affairs was created with the aim of advancing and improving telephone connections, the transmission of radio and television signals, and perhaps the most notable in the scientific field, the creation of nano-satellites for observation, which have made an important contribution in the development of various operations, allowing to maintain the security of the population in a wider space [69]. In this sense, in 2018, the launch of CUBESAT FAC-SAT1 was carried out, with the objective of sending satellite images of the Colombian territory, taken through a camera with a resolution of 30 meters per pixel, thus contributing towards the evaluation and monitoring of the country, in addition to urban development and early attention to natural disasters (FACSAT-1, 2019). Subsequently, the launches of FAC-SAT2 and 3 are planned, with the objective of improving the capacities of size, observation, communication and surveillance with more precise images with a resolution of 5 meters [70].

3.6. The Internet of Things (IoT)

The rapid development of electronic components with the ability to connect to the Internet has made the way of transmitting data over the network much more sophisticated but relatively easy to perform. These components are generally known by the term IoT. Some examples of existing IoT systems are autonomous vehicles (SDVs), micro networks for distributed energy resources systems and drones of surveillance systems for smart cities [71]. Currently it is estimated that there are close to 40 billion IoT devices connected to the network, and by 2025 the amount is estimated to increase to a number between 80 and 120 billion, producing just over 180 billion gigabytes of data that must be stored and analyzed through Big Data techniques and by ML to obtain valuable knowledge in multiplex sectors of society [72].

3.6.1. IoT in public safety

Smart cities are multiplying due to the proliferation of low-cost IoT devices that are capable of continuously generating large data to better understand how a city works, allowing for cost optimization and facilitating monitoring and control of municipal functions such as parking, parking transit, lighting, safety and environmental management [73]. For example, scanning devices with the help of AI algorithms can detect objects and discern their shape, even if they are hidden from the naked eye, and determine if these objects are dangerous and inform the authorities. Also, monitoring systems installed on pedestrian bridges can ensure that they are always optimally loaded to ensure the safety of people. Transportation can be made safer through the issuance of IoT-enabled tickets, making them more secure and easily scannable by incorporating RFID technology, such as those used for the 2018 FIFA World Cup, which helped accelerate the process of Ticket verification despite the large volume of fans without compromising security [74]. In health systems, medical IoT devices can transmit the patient's vital signs to a secure platform where they are stored and analyzed, providing special attention to patients with chronic and elderly diseases [75].

3.6.2. Risks

The industry is changing rapidly and new cases of IoT use are maturing. More and more functionality is being added to IoT systems to obtain the first market advantages and functional benefits, while the safety of IoT system devices is often ignored during design. This is evidenced by recent attacks such as: (1) The US Food and Drug Administration issued safety tips for heart devices about the threat of piracy, and St. Jude Children's Research Hospital patched vulnerable IoT medical devices. (2) Hackers demonstrated a wireless attack on the Tesla Model S car.(3) Investigators hacked Vizio smart TVs to access a home network [76].

IoT devices generally face the same types of cybersecurity and privacy risks as conventional IT devices, although the prevalence and severity of such risks often differ. For example, data security risks are almost always a major concern for conventional IT devices, but for some IoT devices, there may be no data security risks because they do not have any data that needs protection [77], but when talking about vital data, such as temperature sensors, proximity meters, tire pressure or geographic coordinates, it is necessary to protect the IoT device against unwanted interference and establish configurations that do not allow sharing valuable data, such as device georeferencing. This is the case of the US Department of Defense, which urges service members with portable electronic devices to use the strictest privacy settings. The concern comes from a "heat map" released by Strava, creators of a fitness-tracking app that shows the routes that Secret Service members travel in their daily exercises, and which can show military bases and the concentration of the US military personnel abroad [78].

The cyber security of IoT is based on three fundamental security objectives: confidentiality, integrity and availability. To guarantee such objectives, it is essential that the IoT architecture uses methods that protect the data transmitted by the network components. Among the most common methods are: Cryptographic techniques such as encryption and digital signature, Hardware Assurance, Information Security Management Systems (ISMS), IT System Security Assessment and Security Automation and Continuous Monitoring (SACM) [79]. In this last aspect, Telefónica launched the IoT Cybersecurity Unit, a new project in partnership with Subex focused on Internet of Things (IoT) security that combines cybersecurity and IoT. The platform is capable of analyzing traffic with the application of ML algorithms and generates an alert every time it detects a threat that endangers the cybersecurity of the IoT device [80].

4. Discussion

Today's society is experiencing important changes and challenges due to the use of technologies that are increasingly necessary for their daily work and development. Since the creation of MinTIC in 2009, society at a general level has benefited from connectivity projects in areas such as education, health, housing and security. However, much remains to be improved and implemented. In sectors such as technology, there are still remote cities and towns where services such as the Internet are deficient or non-existent, which hinders educational processes, medical care or public order. In addition, the low budget that is historically allocated to the science, technology and education sector make the outlook regular for these areas, although the year 2019 marked an important and hopeful milestone, since, for the first time, Education and Science have the highest percentage of resource allocation, which suggests a promising outlook for the country's future.

5. Conclusions

the research demonstrated that in order to be a competitive society in the technology sector and provide benefits and security guarantees to citizens, it is preponderant to increase the resources destined to offer study and specialization opportunities to Information Technology professionals, in addition to increasing the implementation of new technologies throughout the country. Currently, computer training for high school students is still lacking, mainly because non-professional teachers in technology areas lack the specialized knowledge necessary to face this new wave. In terms of university education, the training options are quite limited, most likely due to the economic factor and the low academic offer of the universities in Cybersecurity studies, data analysis or Artificial Intelligence; one of the biggest obstacles to continue with postgraduate studies.

On the other hand, the security sector is perhaps one of the most promising, perhaps because historically it has had the highest percentage of allocation of the national budget. These institutions are increasingly committed to the implementation of technologies that allow them to carry out their constitutional mission effectively and forcefully. As is evident, there are currently many tools and others are in development, all with the aim of improving strategic decision-making to prevent and protect citizens from events that disturb public order. The modernization of the police and military institutions in Colombia is evident. Research and development of new technologies are present in the vast majority of government entities, as well as in the security sector. With the post-conflict and Colombia being one of the largest drug producing countries, the use of technologies such as drones and nano satellites becomes a fundamental tool for the Police, the Army and the FAC to combat this scourge in security operations, allowing for a broader vision of the national territory without endangering the lives of uniformed men. It should be noted that, although it is true that great progress has been made, it is also important to continue advancing in the creation and updating of laws that protect the privacy of citizens, highlighting new trends such as the use of drones, Big Data and IoT, as well as in the continuous training of the personnel in charge of operating all these technologies.

6. References

1. E. Hernández, N. Duque and C. Moreno, "Big Data: una exploración de investigaciones, tecnologías y casos de aplicación," TecnoLógicas, vol. 20, no. 39, 2017.[Online]. Available: http://www.scielo.org.co/pdf/teclo/v20n39/v20n39a02.pdf

2. U. Sivarajah, M. Mustafa, Z. Irani, and V. Weerakkody, "Critical analysis of Big Data challenges and analytical methods," *Journal of Business Research,* vol., 70, pp. 263-286, 2017, doi: https://doi.org/10.1016/j.jbusres.2016.08.001

3. A. Peña, "Modelo para la Caracterización del Delito en la Ciudad de Bogotá, Aplicando Técnicas de Minería de Datos Espaciales", Tesis de Maestría. Universidad Distrital Francisco José de Caldas. Bogotá, Colombia, pp. 28-35,2017. [Online]. Available: http://repository.udistrital.edu.co/bitstream/11349/6519/1/Pe%C3%B1aSuarezAlfonso2017.pdf

4. R. Pinto, M. Hernández, C. Pinzón, D. Díaz and J. García, J, "Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad. Aplicación de OSINT en un contexto colombiano y análisis de sentimientos," *Revista Vínculos: Ciencia, Tecnología y Sociedad*, vol. 15, no. 2, pp. 195-214, 2018. [Online]. Available: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/13504/14315

5. J. Luo, J. Liu, K. Yang and X. Fu , "Big Data research guided by sociological theory: a triadic dialogue among big data analysis, theory, and predictive models," *The Journal of Chinese Sociology,* vol. 6, no. 11., 2019, doi:https://doi.org/10.1186/s40711-019-0102-4

6. Elpais.com.uy, "Policía de Chicago usa Big Data para evitar crímenes antes de que ocurran," Periódico el País de Uruguay. 2017. [Online]. Available: https://www.elpais.com.uy/vida-actual/policia-chicago-big-data-evitar-crimenes-ocurran.html

7. Prnewswire, "Big Data and Artificial Intelligence to Enhance Homeland Security and Public Safety Technologies," *Revista PR Newswire,* 2019. [Online]. Available: https://www.prnewswire.com/news-releases/big-data-and-artificial-intelligence-to-enhance-homeland-security--public-safety-technologies-300819323.html

8. CONPES 3854, "Documento CONPES 3854. Política Nacional de Seguridad Digital". Biblioteca digital Cámara de Comercio de Bogotá, pp. 12-13, 2016. [Online]. Available: http://hdl.handle.net/11520/14856

9. MinTIC, “Lo que usted debe saber del CONPES de Seguridad Digital”. Ministerio de Tecnologías de la Información y las Comunicaciones, 2016.[Online]. Available: https://www.mintic.gov.co/portal/604/w3-article-15410.html

10. Semana, “Tecnología para saber dónde y cuándo ocurrirá un crimen”. Revista Semana, 2016. [Online]. Available: https://www.semana.com/tecnologia/articulo/aplicaciones-que-predicen-los-crimenes/498979

11. Semana, “La ciberdefensa en Colombia, el nuevo frente de la guerra”. Revista Semana, 2018. [Online]. Available: https://www.semana.com/contenidos-editoriales/fuerzas-armadas-marcha-hacia-la-paz/articulo/la-ciberdefensa-en-colombia/574813

12. B. Balachandran and S. Prasad, “Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence,” *Procedia Computer Science,* vol. 112, pp. 1112-1122, 2017, doi: https://doi.org/10.1016/j.procs.2017.08.138

13. M. Stevens, R. Wehrens and A. De Bont, “Conceptualizations of Big Data and their epistemological claims in healthcare: A discourse analysis,” *Big Data and Society,* vol. 5, no. 2, 2018, doi: https://doi.org/10.1177/2053951718816727

14. Y. Zhang, T. Huang and E. Bompard, “Big data analytics in smart grids: a review,” *Energy Informatics,* vol. 1, no. 8, 2018, doi: https://doi.org/10.1186/s42162-018-0007-5

15. D. Gupta and R. Rani, “A study of big data evolution and research challenges,” *Journal of Information Science,* vol. 45, no. 3, pp. 322-340, 2018, doi: https://doi.org/10.1177/0165551518789880

16. F. Almeida, “Benefits, Challenges and Tools of Big Data Management,” *Journal Of Systems Integration,* vol. 8, no. 4, 2017. [Online]. Available: http://www.si-journal.org/index.php/JSI/article/viewFile/311/317

17. Nascio, “State cio Top 10 Priorities. Strategies, Management and Process Solutions”. 2019. [Online]. Available: https://www.nascio.org/Portals/0/Publications/Documents/2019/NASCIO_Top10_lettersize.pdf

18. Emcien, “Big Data for Public Safety: 4 use cases for intelligence and law enforcement agencies to leverage Big Data for crime prevention”. 2018. [Online]. Available: http://emcien.com/res_guides/Big-Data-for-Public-Safety.pdf

19. L. Shihua, “Shenzhen Uses ‘Video + Big Data’ for Safer City”. Huawei. 2017. [Online]. Available: https://e.huawei.com/en/publications/global/ict_insights/201711060837/public/201712280841

20. T. Hodge, “Application of Big Data Analytics to Support Homeland Security Investigations Targeting Human Smuggling Networks”. Thesis. Naval Postgraduate School, Monterey, California. pp. 45-52, 2018. [Online]. Available: https://www.hsdl.org/?viewanddid=811315

21. D. Van Puyvelde, S. Coulthart and M. Hossain, “Beyond the buzzword: big data and national security decision-making,” *International Affairs,* vol. 93, no. 6, pp. 1397–1416, 2017, doi: https://doi.org/10.1093/ia/iix184

22. M. Favaretto, E. De Clercq and B. Elger, “Big Data and discrimination: perils, promises and solutions. A systematic review,” *Journal of Big Data,* vol. 6, no. 12, 2019, doi: https://doi.org/10.1186/s40537-019-0177-4

23. Parlamento Europeo, “Implicaciones de los macrodatos en los derechos fundamentales. Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI))”. pp. 9-12, 2017. [Online]. Available: http://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.pdf

24. J. Castañeda, L.Mora, C. Botero, A. Toledo and S. Labarthe, “Big Data: Un aporte para la discusión de la política pública en Colombia”. pp. 12-17, 2016. [Online]. Available: https://web.karisma.org.co/wp-content/uploads/download-manager-files/%20BigData_un_aporte_para_la_%20discusion_de_la_politica_publica_en_Colombia.pdf

25. N. Majaj and D. Pelli, “Deep learning-Using machine learning to study biological vision,” *Journal of Vision,* vol. 18, no. 2, 2018, doi: https://doi.org/10.1167/18.13.2

26. F. Osisanwo, J. Akinsola, O. Awodele, J. Hinmikaiye, O. Olakanmi and J. Akinjobi, “Supervised Machine Learning Algorithms: Classification and Comparison,” *International Journal of Computer Trends and Technology* (IJCTT), vol. 48, no. 3, pp. 128-138. 2017. [Online]. Available: https://www.ijcttjournal.org/2017/Volume48/number-3/IJCTT-V48P126.pdf

27. S. Shalev-Shwartz and S. Ben-David, “Understanding Machine Learning: From Theory to Algorithms”. Cambridge University Press. United States of America. pp. 7, 2014. [Online]. Available: https://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning/understanding-machine-learning-theory-algorithms.pdf

28. I. Sarker, A. Kayes and P. Watters, "Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage," *Journal of Big Data,* vol. 6, no.57, 2019, doi: https://doi.org/10.1186/s40537-019-0219-y

29. S. Das, A. Dey, A. Pal and N. Roy, "Applications of Artificial Intelligence in Machine Learning: Review and Prospect," *International Journal of Computer Applications, vol.* 115, no. 9, pp. 31-41, 2015. [Online]. Available:https://research.ijcaonline.org/volume115/number9/pxc3902402.pdf

30. C. Pellerin, "Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges". U.S. Dept of Defense. 2017. [Online]. Available: https://www.defense.gov/Newsroom/News/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/

31. CRS, "Artificial Intelligence and National Security". Congressional Research Service. R45178, Version 4. pp. 15. 2019. [Online]. Available: https://fas.org/sgp/crs/natsec/R45178.pdf

32. P. Goldstein, "How Pattern Recognition and Machine Learning Helps Public Safety Departments," *State Tech Magazine.* 2019. [Online]. Available: https://statetechmagazine.com/article/2019/05/how-pattern-recognition-and-machine-learning-helps-public-safety-departments-perfcon

33. M. Sisak, "NYPD says its new software is helping analysts track crime patterns more quickly". Los Ángeles Times. 2019. [Online]. Available: https://www.latimes.com/nation/la-na-new-york-computer-policing-20190310-story.html

34. E. Hatleback, "The protoscience of cybersecurity," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology,* vol. 15, no. 1, pp. 5-12, 2018, doi: https://doi.org/10.1177/1548512917737635

35. Cisco, "Defensa contra las amenazas más graves de la actualidad". Informe sobre amenazas. Febrero de 2019. Cisco. pp. 5-12, 2019. [Online]. Available: https://www.cisco.com/c/dam/global/es_es/assets/pdfs/es_cybersecurityseries_thrt_01_0219_r2-2.pdf

36. A. Subroto and A. Apriyana, "Cyber risk prediction through social media big data analytics and statistical machine learning," *Journal of Big Data,* vol. 6, no. 50, 2019, doi: https://doi.org/10.1186/s40537-019-0216-1

37. Presidencia de Colombia, "Prevención cibernética". 2017. [Online]. Available: http://especiales.presidencia.gov.co/Documents/20170601-ataques-ciberneticos/sin-ciber-ataques.html

38. AGCS, "Allianz Risk Barometer 2019: Cyber joins business interruption as a leading global risk for companies for first time". Allianz Global Corporate and Specialty. 2019. [Online]. Available: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2019.html

39. Caivirtual, "Costos del Cibercrimen en Colombia 2016-2017". Centro cibernético policial. pp. 1-8, 2017. [Online]. Available: https://caivirtual.policia.gov.co/sites/default/files/costos_del_cibercrimen_v4.pdf

40. Portafolio, "El secuestro de información desangra a las empresas del país". Revista Portafolio. 2019. [Online]. Available: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

41. Deloitte, "Ciber Riesgos y Seguridad de la Información en América Latina and Caribe Tendencias 2019. Reporte Colombia". Deloitte. pp. 1-39, 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Cyber%20Survey%20LATAM%20-%20Colombia%20v2.pdf

42. El Tiempo, "Cibercriminales ponen la mira en sectores de consumo masivo". Periódico El Tiempo. 2019. [Online]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/sectores-de-consumo-masivo-en-la-mira-de-cibercriminales-386806

43. Semana, "Así está Colombia en el ranking de ciberseguridad mundial," Revista Semana. 2019. [Online]. Available: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

44. A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity,* vol. 2, no. 20, 2019, doi: https://doi.org/10.1186/s42400-019-0038-7

45. Y. Hu, A. Yang, H. Li, Y. Sun and L. Sun, "A survey of intrusion detection on industrial control systems," *International Journal of Distributed Sensor Networks,* vol. 14, no. 8, 2018, doi: https://doi.org/10.1177/1550147718794615

46. El Espectador, "Seguridad informática, una guerra de robots". Periódico El Espectador. 2018. [Online]. Available: https://www.elespectador.com/tecnologia/seguridad-informatica-una-guerra-de-robots-articulo-742986

47. P. Rodríguez and A. Cordero, "Ciberseguridad: los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China". Tesis. Universidad de la Salle, Facultad de Ciencias Económicas y Sociales, Bogotá, Colombia. pp. 5-10, 2018. [Online]. Available: https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1083&context=negocios_relaciones

48. Caivirtual, "Amenazas del Cibercrimen en Colombia 2016-2017". Centro cibernético policial. pp. 3-15, 2017. [Online]. Available: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017_1.pdf

49. Portafolio, "Colombia y Chile, con memorando de ciberseguridad". Revista Portafolio, 2019. [Online].Available:https://www.portafolio.co/negocios/colombia-y-chile-con-memorando-de-ciberseguridad-527823

50. Presidencia de Colombia, "Convenio sobre la Ciberdelincuencia-Ley 1928 del 24/jul/2018. Colombia aprueba la adhesión a convenio Budapest o convención de Europa sobre cibercriminalidad", pp. 6-49,2018. [Online]. Available: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

51. Caivirtual,"Balance cibercrimen en Colombia 2017". Centro cibernético policial, 2017. pp. 2-10, 2017. [Online]. Available: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

52. F. Catota, M. Morgan and D. Sicker, "Cybersecurity education in a developing nation: the Ecuadorian environment," *Journal of Cybersecurity,* vol. 5, no. 1, pp. 1-19, 2019, doi: https://doi.org/10.1093/cybsec/tyz001

53. Presidencia de Colombia, "Gobierno y Cisco firmaron acuerdo para la innovación y transformación digital de Colombia". 2019. [Online]. Available: https://id.presidencia.gov.co/Paginas/prensa/2019/190508-Gobierno-y-Cisco-firmaron-acuerdo-para-la-innovacion-y-transformacion-digital-de-Colombia.aspx

54. G. Rosser and T. Cheng, "Improving the Robustness and Accuracy of Crime Prediction with the Self-Exciting Point Process Through Isotropic Triggering," *Applied Spatial Analysis and Policy,* vol. 12, no. 1, pp. 5–25. 2019, doi:https://doi.org/10.1007/s12061-016-9198-y

55. F. Coppola, "Mapping the Brain to Predict Antisocial Behaviour: New Frontiers in Neurocriminology, 'New' Challenges for Criminal Justice," *UCL Journal of Law and Jurisprudence – Special,* vol. 1, no. 5, pp. 1-24, 2018.[Online]. Available: https://discovery.ucl.ac.uk/id/eprint/10045129/1/Federica%20Coppola.pdf

56. G. Mohler and M. Porter, “Rotational grid, PAI-maximizing crime forecasts.Statistical Analysis and Data Mining,”*The ASA Data Science Journal,* vol. 11, no. 5, pp.227-236, 2018. [Online]. Available: https://docs.wixstatic.com/ugd/9226cc_0a3ab606687b47788f7fdb3926d0bfaf.pdf

57. G. Saltos and M. Cocea, “An Exploration of Crime Prediction Using Data Mining on Open Data,” *International Journal of Information Technology and Decision Making,* vol.16, no. 5, pp. 1155-1181, 2017. [Online]. Available: https://www.researchgate.net/publication/317134535_An_Exploration_of_Crime_Prediction_Using_Data_Mining_on_Open_Data

58. M. Smith, “Can we predict when and where a crime will take place?”. BBC News. 2018. [Online]. Available: https://www.bbc.com/news/business-46017239

59. IBM, “Crime Prediction and Prevention”. IBM Public Safety and Policing. [Online]. Available: https://www.ibm.com/industries/government/public-safety/crime-prediction-prevention

60. BBC, “El ladrón que fue atrapado en Italia gracias a un nuevo algoritmo para predecir delitos inventado en Nápoles”. BBC News. 2018. [Online]. Available: https://www.bbc.com/mundo/noticias-46261759

61. K. Gurney, “Using Data to Predict and Prevent Crime in LatAm,” *Revista Insight Crime.* 2015. [Online]. Available: https://www.insightcrime.org/news/analysis/using-data-to-predict-and-prevent-crime-in-latam/

62. Unesco, “Cómo los datos y las TIC pueden ser eficaces aliados para prevenir la violencia juvenil en los países del norte de Centroamérica”. *UNESCO,* pp. 7-28, 2018. [Online]. Available: http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Montevideo/pdf/PolicyPapers-NorteCentroAmerica-TICViolenciaJovenes-web-.pdf

63. Alcaldía de Bogotá, “Bogotá desarrollará un método de predicción de delitos”. Alcaldía de Bogotá.2019.[Online].Available:https://bogota.gov.co/mi-ciudad/seguridad/nuevo-metodo-de-prediccion-de-delitos-sera-desarrollado-en-bogota

64. SCJ, “Bogotá, pionera en el país en desarrollar un método de predicción de delitos”. Secretaría Distrital de Seguridad, Convivencia y Justicia. 2019. [Online]. Available: https://scj.gov.co/es/noticias/bogot%C3%A1-pionera-pa%C3%ADs-desarrollar-m%C3%A9todo-predicci%C3%B3n-delitos

65. C. Armour and J. Ross, “The Health and Well-Being of Military Drone Operators and Intelligence Analysts: A Systematic Review,” *Military Psychology,* vol. 29, no. 2, pp. 83–98. 2017, doi: https://doi.org/10.1037/mil0000149

66. Revista Policía Nacional, “Nº. 317 Cuarta Edición Octubre-Diciembre 2018”. pp. 34-42, 2018. [Online]. Available: https://www.policia.gov.co/sites/default/files/publicaciones-institucionales/revista-policia-nacional-edicion-317.pdf

67. J. Rodríguez, “Entran en operación los drones para vigilancia en Bogotá”. RCN Radio. 2019. [Online]. Available: https://www.rcnradio.com/bogota/entran-en-operacion-los-drones-para-vigilancia-en-bogota

68. P. Deschênes, “The Rise of the Drones: Technological Development of Miniaturised Weapons and the Challenges for the Royal Canadian Navy,” *Canadian Military Journal,* vol. 19, no. 2, pp. 1-6, 2019. [Online]. Available: http://www.journal.forces.gc.ca/Vol19/No2/PDF/CMJ192Ep51.pdf

69. SIC, “Boletín Tecnológico Nanosatélites. Centro de Información Tecnológica y Apoyo a la Gestión de la Propiedad Industrial (CIGEPI)”. Superintendencia de Industria y Comercio. pp. 1-82, 2017. [Online]. Available: http://www.sic.gov.co/sites/default/files/files/Propiedad%20Industrial/Boletines_Tecnologicos/Boletin_Nanosatelites.pdf

70. FACSAT-2, “Así avanza el ensamblaje del prototipo del FACSAT-2”. Fuerza Aérea Colombiana. 2019. [Online]. Available: https://www.fac.mil.co/as%C3%AD-avanza-el-ensamblaje-del-prototipo-del-facsat-2

71. M. Mohamad and W, Hassan, “Current research on Internet of Things (IoT) security: A survey,” *Computer Networks,* vol. 148, pp. 283-294, 2019, doi: https://doi.org/10.1016/j.comnet.2018.11.025

72. S. Balakrishna, M. Thirumaran and V. Kumar Solanki, “Machine Learning based Improved Gaussian Mixture Model for IoT Real-Time Data Analysis,” *Revista Ingeniería Solidaria,* vol. 16, no. 1, pp. 1-30, 2020, doi: https://doi.org/10.16925/2357-6014.2020.01.02

73. N. Alban, “El Internet de las Cosas para un Gobierno Inteligente”. *Alianza CAOBA,* 2019. [Online]. Available: http://alianzacaoba.co/inicio/mas-noticias-big-data-y-data-analytics-en-colombia-y-el-mundo/internet-las-cosas-gobierno-inteligente/

74. N. Joshi, “Leveraging AI And IoT For Citizen Security In Smart Cities,” *Revista Forbes.* 2019. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/07/09/leveraging-ai-and-iot-for-citizen-security-in-smart-cities/#455f82eae151

75. H. Mohammed and M. Qayyum, “Internet of Things: A Study on Security and Privacy Threats,” *IEEE,* 2017, doi: 10.1109/Anti-Cybercrime.2017.7905270

76. H. Patel, “IoT Needs Better Security,” *ISACA Journal,* vol. 3, pp. 1-5, 2017. [Online]. Available: https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/iot-needs-better-security.aspx

77. K. Boeckl, M. Fagan, M, and W. Fisher, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” *National Institute of Standards and Technology.* NISTIR 8228. pp. 1-35, 2019, doi: https://doi.org/10.6028/NIST.IR.8228

78. J. Garamone, “DoD Studying Implications of Wearable Devices Giving Too Much Info”. U.S. Department of Defense. 2018. [Online]. Available: https://dod.defense.gov/News/Article/Article/1426579/dod-studying-implications-of-wearable-devices-giving-too-much-info

79. NISTIR 8200, “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things”. (IoT). National Institute of Standards and Technology. pp. 24-44, 2018, doi: https://doi.org/10.6028/NIST.IR.8200

80. Telefónica, “Telefónica velará por la seguridad de Internet de las Cosas con una nueva unidad de ciberseguridad IoT”. Telefónica, 2019. [Online]. Available: https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-velara-por-la-seguridad-de-internet-de-las-cosas-con-una-nueva-unidad-de-ciberseguridad-iot