DOI: 10.53477/2668-2001-21-13

CHALLENGES AND OPPORTUNITIES FOR INTELLIGENCE SERVICES IN THE CONTEXT OF TECHNOLOGICAL DEVELOPMENTS AND INFORMATION OVERLOAD

Robert Călinoiu[1]
"Carol I" National Defence University

Abstract

Intelligence has been one of the first professions in the World existence, due to the human nature of permanent desire of progress and possession. Its evolution has been marked by various developments, out of which technology seems to have the greatest impact. While advanced technology has made the overall cycle of life faster and better, it has also diversified the challenges to many professions, intelligence being one of them. Adapting to the ever evolving realities, intelligence has to transform the challenges in opportunities and advance the national interests of security at national and international levels.

Keywords: intelligence; challenge; opportunity; information overload; technological development; collection; analysis.

INTRODUCTION

For the most part of the history, intelligence collection had been made through the effort of spies, who openly observed enemy's maneuvers and acquired illegally documents of interest, informing directly their superiors. Later on, when the enemy's communications were coded, methods of interception and decoding were developed. Transmitted on paper or via technical means, the messages of interest were targeted and then decoded for the political or military use.

In the last two hundred years, while the technology developed in an accelerated manner, often in lead being the military research, sophisticated means of collection and transmission, as well as capabilities for interception and decoding were developed in a continuous and competitive cycle.

Analyzing the history of intelligence, we could infer that along with the World Wars and the fall of the Berlin wall, the period of swift technological progress of the years 2000 greatly influenced the domain.

METHODOLOGY

Our approach in addressing the subject is a three-step one. First, we will analyze the technological developments influencing the intelligence field along the history.

The second step is presenting the challenges and opportunities caused by the information overload upon the intelligence, and its impact in reaching the specific goals in the domain.

Finally, we will draw a few conclusions concerning the current situation, hopping in contributing to creating a clearer picture of the intelligence realm, being on the same time aware that within the existing limits of the Conference proceedings the subject would be far from being exhausted.

TECHNOLOGICAL DEVELOPMENTS EFFECT ON INTELLIGENCE

The First World War brought the first uses of technology in the field of intelligence. Thus, the installation of cameras on aerial means allowed the creation of images that provided clues to the disposition or movement of enemy troops (Missouri S&T 2004). Interception of enemy

[1] Corresponding author: robert.calinoiu@eeas.europa.eu

communications was also used successfully. The British interception of the German Foreign Ministry's telegrams to their representative in Mexico, who was instructed to promise the accreditation state the recovery of lost American territories if it entered the war on the German side and attacked the United States, accelerated the entry of US in the fight (Loch K. Johnson 2007).

In World War II, aerial photography was widely used both to identify targets and to assess their impact after hitting, as precision bombing was a non-existent concept and quantity replaced quality, with devastating effects on the civilian population and infrastructure (Missouri S&T 2004).

Technological progress on that period has allowed the development of communications encryption and decryption equipment. Thus, the ability of the British army to decipher the messages sent by the German encryption machine Enigma (Crypto Museum 2021) allowed achieving essential successes both in land battles, but especially in naval battles in the Atlantic Ocean. Equally, the US military's decoding of Japanese coded communications won the Battle of Midway, which marked a turning point in tipping the balance of victory over the Americans in the Pacific (Hystory.com 2019).

The Second World War also caused the emergence of two new forms of collection, Electronic Intelligence (ELINT) and intelligence by measuring technical parameters (Measurement Intelligence - MASINT). The first example of ELINT was the determination of the emissions of the Japanese radars, whose period of operation was associated with the missions that the aviation was to carry out, constituting an indication of alerting the American aviation and anti-aircraft means (Jeffrey 2007). In the field of MASINT, the collection of data such as the level of chemicals in the waters around the German military facilities indicates an increase in the production of bombs or projectiles and the imminence of the execution of a new offensive plan (Jeffrey 2007).

During the Cold War, the advent of satellites allowed the development of Imagery Intelligence (IMINT). The images were vital in the determination by the two superpowers, the USA and the Soviet Union, of the number of intercontinental ballistic missiles held by the competing state, of the technique capable of using this type of weapon (fixed ground facilities, mobile means, submarines, later aviation), as well as their characteristics. Mutual knowledge of these capabilities led to the conclusion of an arms control agreement - *Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems* (US Department of State 1972), with each party having the certainty that it could verify a possible breach, and an increase in the number of means of striking the other party no longer had military or economic reasons, as each would he could have completely destroyed his opponent several times with the existing ones.

Technological progress has had a major impact on the transformation of the military intelligence field throughout its existence, but the greatest influence has been felt since the 2000s, when innovations in communications and imagery[2] have experienced great dynamics. The Internet has spread to almost the entire globe, offering increasing speeds and capacities for uploading or downloading written, audio or video files.

The development of the Internet has allowed the development of applications, such as social networks. The largest of them (established in 2004), Facebook, had on 23 October 2020 a number of 2,701,000,000 accounts (Statista 2020). All these networks mean as many databases, ready to be used for positive or evil purposes. In accessing the internet, it has gone from the cable connection, from the 90's, to the wireless connection, with faster and faster speeds of loading or downloading data.

The year 2020 marked the emergence of 5G communications networks, which will provide such a high speed of data transmission (Qualcomm 2021) that it will make it possible to exchange them in real time, in large volumes and almost total digitization of the industry. Of course, the increase in the volume of data will be followed by the need to store them, in specially designed servers (in the "cloud"), or in their own servers, to maintain full confidentiality.

[2] Imagery Analysis is the thorough process of detection, recognition, identification and interpretation (analysis) of objects/terrain/situations on imagery. The determination of their significance and implications in the geographic area in which they are imaged are primal. Analysis is accomplished according to the NATO Standard (STANAG 3596) Reconnaissance Reporting method, comprising of 19 Categories. In doing this, all aspects of a location of interest or a potential object may be described properly and completely. Source http://www.vigilance.nl/imagery-analysis.html; details in AAP- 6, NATO Glossary of Terms and Definitions, NATO Standardization Agency (NSA), 2019), source: file:///C:/Users/icalinro/AppData/Local/Temp/AAP-06%202019%20EF.pdf, accessed on 27 February 2021

However, technological developments involve, in addition to economic and financial competition, aspects of national or international security. Thus, the development of 5G technology by China and its willingness to implement it through Huawei in various countries around the world, led to fears that it could be used for espionage purposes (Rubio 2020). For this reason, countries such as the USA, Great Britain, France or Singapore have forbidden local companies to cooperate with Huawei for the development of 5G networks. On 21.10.2020, Sweden also joined the countries banning the use of Huawei or Zhongxing Telecommunications Equipment – ZTE technology, motivating the recommendation of military intelligence and security services and asking local telecommunications companies to replace, by 2025, any equipment of the above-mentioned Chinese companies in network infrastructure on the territory of Sweden (Tiezii 2020).

Thus, if 20 years ago to intercept a phone a person or a team were needed to install a physical device in a phone or on the phone line, and for these activities to be legal you needed a court order, now the intelligence services can intercept almost any call just by activating specialized equipment thousands of kilometers away from the target.

Disputes over the legality of such actions are usually resolved after the technology has evolved again, and the activity that can be incriminated no longer needs to be performed, the cycle repeating itself. According to some theorists (Johnson 2007), at this point it is easier to record all telephone conversations and use specialized search programs in the database thus created, using keywords to discover information of interest, than to make efforts to find clues, which then to or used to obtain warrants for targeted listening, for a limited time, to a target telephone.

Currently, the more technologically connected you are to the world around you, the more vulnerable you are to exposing activities.

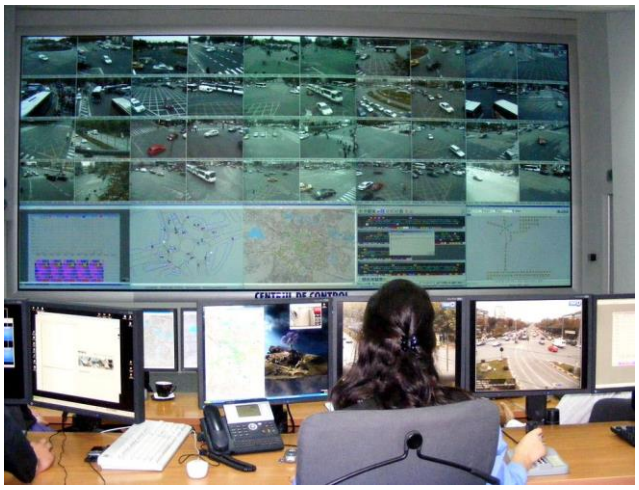

Figure1. Bucharest Surveillance Command Center
Source: Libertatea, 10 June 2018

And it's not just about intercepting communications, but also other aspects, such as video camera systems in big cities, which are usually connected to the network using wireless internet, thus theoretically allowing signal interception. Increasing the number of monitoring cameras is undoubtedly a positive aspect of ensuring the security of a nation, but it can also be destructive in the case of the use of information by enemy organizations or individuals[3]. In addition, the diversity of entities that install video surveillance cameras in a city without centralized coordination makes it possible for such a network to be set up by an organization with malicious interests, or to interfere with well-intentioned but unprotected systems due to the lack of a decent security culture, describing the technical characteristics in detail[4]. In Photo 1 is shown the Bucharest Surveillance Center, where the journalists from Libertatea apparently entered and took photos without any restrictions.

In addition to intercepting communications, devices containing Global Positioning System (GPS) applications such as phones, tablets, or smart watches can track or trace a person's route. Although seemingly harmless, it has been demonstrated that an inventive mind can turn an

[3] According to the Article "Bucharest is monitored with over 1,700 surveillance cameras", from the newspaper *Libertatea*, 10 June 2018 Edition, in Bucharest at that time there were at least 1,709 surveillance cameras belonging to the six Districts of the Capital, adding to the 302 owned by the City Hall. Source: *https://www.libertatea.ro/stiri/bucurestiul-este-monitorizat-cu-peste-1-700-de-camere-de-supraveghere-2286127*, accessed on 28 February 2021.

[4] Such examples can be found in Bucharest at the following links: *http://www.netcam.ro/network/imagini/camere-web-live/webcams-din-zona-bucuresti.html* – set up for touristic purposes, and *https://adp-sector1.ro/proiecte/sistem-metropolitan-de-supraveghere-video/*meant for surveilling the Public Parks in the 1st District, having 703 video cameras. Accessed on 28 February 2021

application developed for positive purposes, such as monitoring health parameters, into one designed to achieve precise military goals.

In this respect, the site Bellingcat showed how the fitness application and monitoring of physical parameters "Polar", installed on smart devices such as watches or medical bracelets, can uncover military bases, headquarters of intelligence agencies, military airfields, nuclear weapons storage sites, secret bases or diplomatic missions (Postma 2018).

Thus, the application also functions as a social platform, where personal data is downloaded for comparison (similar to two other applications, Garmin and Strava). By overlapping the data, both the duration and performance of the physical exercises and the routes where these exercises take place are disclosed, connecting the bases where the soldiers run with their homes or places of stationing in external missions. Often, the data is connected to the information on Facebook, even if the user did not make this connection personally, but failed to set up electronic devices and computer applications so that they do not do it automatically. Some platforms do not allow access to the data of other people using the same application, while others allow access to the history since its launch (provided it has been used since that date), in the case of Polar, from 2014.

Analysing in an unauthorized manner (due to a product security vulnerability) the data on the Polar platform, Bellingcat site experts were able to profile more than 6,500 users, military or civilian, American or other nationalities, working in the Armed Forces or intelligence services in Naval stations, Army or Air bases, the Federal Bureau of Investigation (FBI) or the National Security Agency (NSA), located in Guantanamo Bay (American base in Cuba), Crimea, Baghdad, Afghanistan or South Korea (Postma 2018).

Another application that can be used extensively for espionage purposes, recently developed (2006), is Waze. It was originally developed in Israel (European Patent Office 2008), the previous name being "FreeMap Israel". Taken over and developed by Google in June 2013, the app has about 130 million monthly users, and is available in 50 different languages. The application is based on the free collection of travel data and traffic values from users, which can report accidents, traffic jams, delays compared to normal values on certain routes, optimal travel routes, maximum permissible speeds, real average speeds, the nearest objectives of interest (fuel stations, pharmacies, hospitals, police stations, etc.).

Waze offers the recognition of a route for an intelligence officer without him exposing himself by going out on the field. By combining the Waze application with other applications such as Google Earth, maps can be created that include images at the level of travel routes. In 2014, Waze launched the Connected Citizens Program (CCP), which allows two-way data exchange free, a program currently used by 450 government organizations, ministries of transport, municipal companies that analyze traffic or emergency services (ESRI The Science of Where 2021).

Created for eminently positive purposes, the application can also be used for negative purposes, with major consequences. A demonstration of this was made by two students from the Technion Institute of Technology in Israel in 2014 (Atherton 2014), who created a fake traffic jam using data sent to the Waze application from several thousand fake accounts simulating as many different phones used in traffic, created using a computer program. Thus, they signalled the existence of a blockage on one of the important road arteries in Tel Aviv, blocking the traffic on the side ones. The demonstration and the way of action were sent to the Waze administrators, in order to be able to prevent such cyber-attacks from malicious organizations.

INFORMATION OVERLOAD IMPACT UPON THE INTELLIGENCE

The technological developments, especially the digitalization, has also influenced in a huge manner the information field. From producing it, to transforming the old data into digital formats and the capability of storing vast amounts of information in virtual public libraries or classified servers, doubled by easing the access to almost any piece of information from anywhere on the glob to anyone on the planet, the domain exploded in almost all aspects. Named an Era of Information, the period at the beginning of the 21st Century lives at the level of expectation.

For the intelligence field, easier access to collecting information and transforming it into useful products and knowledge has become a big challenge. From the concept of superiority of information, the specialists moved to the concept of the superiority of knowledge, meaning that the information presented to the decision makers has to be timely, accurate, and actionable. In order to do that, an intelligence service should be able to distinguish the valid information from fake news or disinformation operations of its enemies. Luckily, differentiating between information and intelligence is not a new endeavour, many services (including the Romanian Military Intelligence Directorate) having for decades as logo the owl, a bird able to see in darkness and distinguish its prey from other uninteresting items.

Easy access to collection may lead, sometimes, to a culture of a minimal effort, acquiring and providing information readily available, sometimes not verified from multiple sources. This habit is induced, at times, by leaders of shallow understanding, looking to find rapid confirmation from their intelligence services on what they hear on television or read in the newspapers. The trend was nicknamed “passing on information” and “making educated guesses” by Nick Gurr, former Deputy Chief of the British Defence Intelligence for Analysis and Production in one of the meetings hosted in Brussels by the EU Military Staff Intelligence Directorate, showing that the same challenge exists in many countries.

If the passed on information is taken as a valid fact by a leader and publicly expressed, followed by later denial, it may lead to an unfavourable assessment of lack of competency from a friendly service, with repercussions on the reciprocal trust and cooperation level. Moreover, it may look like a weak organization for an enemy intelligence service, and could be followed by successful disinformation campaigns (as long as everything in open media is taken as valid facts and acted upon).

One of the most disastrous impacts of a disinformation campaign has been the Brexit Referendum. According to multiple sources, some 80.000 posts of the fake Facebook accounts linked to Russian agents have been published in two years prior to the referendum (Gillett 2017). Another source is mentioning an inquiry of the British Parliament on Facebook and Twitter as part of ongoing probes into alleged Russian meddling in the Brexit vote (Ghosh 2017). To add up, according to The New Yorker (Mayer 2018), a US private Big Data company, Cambridge Analytica, obtained millions of people’s personal data from Facebook, without users’ permission, availing them to influence the Brexit campaign by primarily targeting American citizens having relatives in UK.

While probing the meddling of foreign entities in the Brexit referendum is difficult due to the lack of legislation governing the virtual environment, the tight result of 51.89% of the leave vote against 48.11% on the remain vote may be considered the outcome of a concerted mass-media pro leave campaign against a paralyzed safeguarding sense of right and wrong. The results will negatively affect the Union and its member states for a very long period on multiple levels, security being just one, as well as most of the British citizens, starting with those previously working in Brussels in EU institutions.

Coping with information overload may seriously undermine the quality of intelligence. All the documents delivered to an analyst are potentially important, having already met some criteria defining them as relevant to a certain monitored issue. Prioritization is important, but there are known biases, like the tendency to consider the most recent information the most valid one. In addition, when the documentation is vast, the documents read at the beginning are fading away, or the opposite, the understanding of the later ones is impaired by tiredness and, not rarely, stressful environments.

The solution may be the artificial intelligence capable of processing massive quantities of data and rapidly presenting the requested findings. The artificial intelligence may also help eliminating the information duplicated (circular reporting) during the collection process.

Technology is also called to solve the current challenges of the fast revolving cycle of intelligence when it comes to the last component of it, dissemination. After the fast collection and even faster analysis in the intelligence services laboratories, a rapid dissemination of the now intelligence product is required. Being classified, adequate means are requested at both ends, sender and receiver. The reality of nowadays shows that the slightest effort in deciphering a message may

lead to annoyance and avoidance of such messages, being preferred current unclassified “intelligence” products, ready to be made public in the virtual environment, part of a never-ending political campaign. Of course, the case is different with classified strategic intelligence papers, forming the most important part of the existence reason of an intelligence service, and contribution to the knowledge supremacy of a state.

CONCLUSIONS

We appreciate that technological development has led to important changes in the intelligence domain, in all aspects of the intelligence cycle, from management, to collection, to analysis, and finally to dissemination. In addition, it greatly affected the theoretical and practical approach to the training of intelligence officers, the technical qualities being highly sought after today, compared to the desirable psychosocial skills 30 years ago.

We also consider that technology can allow the planning and execution of missions faster than in the past, but also countering the illegal hostile actions. Connecting the facts and events is much easier, which creates additional pressure on intelligence services to deliver faster the desired outcomes.

We emphasize that another consequence of the technological revolution is the overload of information available, from which an intelligence service must have the ability to quickly detect useful information, through computer applications or the effort of professionals, and then deliver information products in a timely manner to decision makers. They, in turn, thanks to the same technological revolution, are overloaded by information from the mass media, some of interest in certain particular situations, and require fast and punctual information that is not related to the usual strategic purpose of an intelligence service. In these circumstances, the reality shows that one falls either in accepting the requests as they are, transmitting information as polite as possible, or structural changes are started to provide answers to contemporary worrying events.

We believe that another major challenge to an intelligence service in the age of technology may be the interruption for a short or a long period of one of its major high-tech components, the Internet. Thus, the growing dependence on the Internet, the digitalization of society, can cause major damage to the general functioning of a state, with major implications on its security in general and citizens in particular, if, for accidental or intentional reasons, its provision is interrupted. Thus, the intelligence services have the obligation to have their own information circuits, which would allow to timely informing the decision makers on classic alternative channels, as in any classic war situation. Although difficult to imagine, the current COVID 19 pandemic shows us that even the most negative scenarios can become a reality in unfavorable contexts.

REFERENCES

Atherton, Kelsey D. 2014. "Israeli Students Spoof Waze App with Fake Traffic Jam." *Popular Science.* March 31. Accessed February 28, 2021. https://www.popsci.com/article/gadgets/israeli-students-spoof-waze-app-fake-traffic-jam/

Crypto Museum. 2021. "Hystory of Enigma." *cryptomuseum.com.* February 27. Accessed February 27, 2021. https://www.cryptomuseum.com/crypto/enigma/hist.htm

ESRI The Science of Where. 2021. "How does ArcGIS work with the Waze Connected Citizens Program (CCP)?" *ESRI.* February 28. Accessed February 28, 2021. https://support.esri.com/en/technical-article/000019662

European Patent Office. 2008. "Waze Patent Registration ." *Espacenet.* August 27. Accessed February 28, 2021. https://worldwide.espacenet.com/patent/search/family/041722029/publication/US8612136B2?q=pn%3DUS8612136

Ghosh, Shona. 2017. "The UK's election watchdog has now questioned Google over Russian meddling in Brexit." *Business Insider.* November 28. Accessed February 28, 2021.

https://www.businessinsider.com/electoral-commission-probe-google-over-russian-meddling-in-brexit-2017-11?r=DE&IR=T

Gillett, Francesca. 2017. "Electoral Commission launches probe into Russian meddling in Brexit vote using Twitter and Facebook." *Evening Standard.* November 02. Accessed February 28, 2021. https://www.standard.co.uk/news/politics/election-watchdog-launches-probe-into-russian-meddling-in-brexit-vote-a3674251.html

Hystory.com. 2019. "Battle of Midway." *Hystory.com.* December 17. Accessed February 27, 2021. https://www.history.com/topics/world-war-ii/battle-of-midway

Jeffrey, Richelson T. 2007. *The Technical Collection of Intelligence.* New York: Routledge

Johnson, Loch K. 2007. *Handbook of Intelligence Studies.* New York: Routledge. Accessed February 28, 2021.

Loch K. Johnson, Wirtz J. James. 2007. *The Evolution of the US Intelligence Community – An Historical Overview.* Vol. Strategic Intelligence. Los Angeles: Rxbury Publishing Company.

Mayer, Jane. 2018. "New Evidence Emerges of Steve Bannon and Cambridge Analytica's Role in Brexit." *The New Yorker.* November 18. Accessed February 28, 2021. https://www.newyorker.com/news/news-desk/new-evidence-emerges-of-steve-bannon-and-cambridge-analyticas-role-in-brexit

Missouri S&T. 2004. "Evolution of Airborne Remote Sensing 1783-1950." *https://www.mst.edu/.* November 04. Accessed February 27, 2021. https://web.mst.edu/~rogersda/gis/Early%20Days%20Remote%20Sensing.pdf

Postma, Foeke. 2018. "fter Strava, Polar is Revealing the Homes of Soldiers and Spies."*Bellingcat.* July 08. Accessed February 28, 2021. https://www.bellingcat.com/ resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

Qualcomm. 2021. *Everything you need to know about 5G.* February 28. Accessed February 28, 2021. https://www.qualcomm.com/5g/what-is-5g

Rubio, Senator Marco. 2020. "Op-ed: America and its allies must reject China's Huawei and lead on 5G development." *CNBC.* September 03. Accessed February 28, 2021. https://www.cnbc.com/2020/09/03/op-ed-america-allies-must-reject-chinas-huawei-lead-on-5g.html

Statista. 2020. *Number of monthly active Facebook users worldwide as of 4th quarter 2020.* December 31. Accessed February 28, 2021. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Tiezii, Shannon. 2020. "Sweden Becomes Latest – and Among Most Forceful – to Ban Huawei From 5G. "*The Diplomat.* October 21. Accessed February 28, 2021. https://thediplomat.com/2020/10/sweden-becomes-latest-and-among-most-forceful-to-ban-huawei-from-5g/

US Department of State. 1972. May-October 26; 3. Accessed February 28, 2021. https://2009-2017.state.gov/t/isn/trty/16332.htm