BUSINESS COUNTERINTELLIGENCE PRACTICES

Horia Mircea BOTOŞ [*]

Gheorghe RADU [**]

Abstract

Counterintelligence, as defined by the Merriam Webster Dictionary, is an organized activity of an intelligence service designed to block an enemy's sources of information, to deceive the enemy, to prevent sabotage, and to gather political and military information. It protects against espionage, assassinations, etc. that might be done by a foreign agent. Likewise, when we think about business, the source of a country's wealth, Business Counterintelligence is an effort of an organization or country to protect its private and hypersensitive information from being unwantedly accessed.

Intelligence refers to the information that supports decision making and sustains strategic developments. Thus counterintelligence is the information used to defend the company from another competitive business and all the implied tools and processes.

Because of this, Competitive intelligence and Business Counterintelligence are considered sometimes synonymous, despite being different. Competitive intelligence is the gathering of information, whereas business counterintelligence is the protecting of the information against the CI efforts. So business counterintelligence represents the actions taken to limit the access of others to the sensitive and actionable information of the company.

In this paper we will identify and structure the term of business counterintelligence and will present examples of such practices. We will try exemplifying the use of counterintelligence in the business sector by presenting, from a theoretical point of view, the Russian approaches on Western companies.

Keywords: *Intelligence, Counterintelligence, Business Intelligence, Business Counterintelligence, Russia*

Theoretical aspects

Counterintelligence (CI) refers to information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations

[*] PhD, Babes Bolyai University DSIIC horia.botos@gmail.com

[**] BA Security Studies, Babes Bolyai University DSIIC, gicu.radu1@gmail.com

or persons or international terrorist activities, but not including personnel, physical, document or communications security programs. [1]

When we speak about *counterintelligence* we should know that this term is divided in three main categories:[2]

1. *Collective counterintelligence* – is responsible for gaining information about an opponent's intelligence collection capabilities whose aim is at an entity.

2. *Defensive counterintelligence* – the thwarting efforts by hostile intelligence services to penetrate other services.

3. *Offensive counterintelligence* – the action of identifying another opponent's efforts against the system, trying to manipulate these attacks by either "turning" the opponent's against into double agents or feeding them with false information.

Also this term is used in more spheres. When we speak about *military counterintelligence,* we should go with our mind to the United Stated Army Counterintelligence that is responsible for the *counterintelligence* activities aimed to detect, identify, assess, counter, exploit and/or neutralize adversarial, foreign intelligence services, international terrorist organizations, and insider threats to the United States Army and U.S. Department of Defence.[3]

We also have *economic counterintelligence.* A good example here is the program initiated by FBI in 1994 which was created to protect the U.S. national security. Kenneth Geide that was the head of the Economic Counterintelligence Unit, explained that one of the methods that foreign governments often use is to hide their economic collection activities within their legitimate activities.[4]

Because of this nature of the Counterintelligence service, it offers a wide array of tactics, techniques and protocols that insure a company's Information security. Such services may include: analysis of vulnerabilities for specialized threats (internal and external to the company), Business operational procedures, Proprietary Information Protective measures, Research and analysis of offensive Business Intelligence Practices.

Business intelligence (BI) refers to the procedural and technical infrastructure that collects, stores and analyses the data produced by a company's activities. Business intelligence is a broad term that encompasses

---

[1] Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR, 1981 Comp., p.1

[2] Lowenthal, M. (2003). Intelligence: From secrets to policy. Washington, DC: CQ Press.

[3] United States Army Regulation 381-20, *The Army Counterintelligence Program*, May 25, 2010

[4] Hedieh Nasheri, Economic Espionage and Industrial Spying, p76

data mining, process analysis, performance benchmarking, descriptive analytics, and so on. Business intelligence is meant to take in all the data being generated by a business and present easy to digest performance measures and trends that will inform management decisions.[5]

Business counterintelligence (business CI) is the collective efforts designed to protect an organization's sensitive information from unauthorized access.[6]

Taking in consideration this definition of Business counterintelligence, we can observe that it is similar to the one of Competitive Intelligence (The process of collecting and analyzing information about competitors' strengths and weaknesses in a legal and ethical manner to enhance business decision-making). Competitive intelligence is the activity responsible for gathering information, whereas business counterintelligence is the activity responsible for the protection of the information against the Competitive Intelligence efforts. So *business counterintelligence* represents the actions taken to limit the access of others organizations to important information that could put the company at a disadvantage if made public. Such information could be: R&D developments, future investments, intellectual property information or M&A's.

Functions and Forces defining Counterintelligence

Our study has evidenced that the general functions in the field of Counterintelligence remain the same regardless of the field of application. The fields of from the perspectives of which the analysis would be are: technological, economic, occupational, spatial and cultural.

The four functions of CI are:

a) operation;
b) investigation;
c) collection and reporting;
d) analysis, production and dissemination.

The CI Operations employ specialized techniques and personnel, and are directed against any espionage, sabotage, subversion or threats. As directed to general activities, Business Counterintelligence covers: counterespionage, counter subversion, counter sabotage and exploitation or neutralization operations. Compared to standard CI, you can observe that there are no mentions of terrorism, as this is generally a referred as unlawful use of violence and intimidation of civilians, in principal, in order to follow a political aim.

---

[5] http://www.investopedia.com/terms/b/business-intelligence-bi.asp
[6] Business Counterintelligence : Sustainable Practice Or Passing Fad?, Shear, Christopher James, accessed at: http://scholar.sun.ac.za/handle/10019.1/1930

CI investigations are the next function, and they cover systematic and detailed inquiries/examination to uncover facts on the matter that is the objective of the operation. The results of these actions are the function of Collection and Reporting, which are intended to identify actual or potential threats. After these functions are done, the next function will be the performing of an analysis on the available data and information, producing the report and afterwards handing in the results.

In Business CI, the protocol is not far off; just the purpose is aligned with the Business needs of an organization in order to protect itself from its competitors. This is why when analyzing the academic materials on Business Counterintelligence you will find many mentions of corporate espionage or corporate counterespionage.

The perspectives initially mentioned are just some of the elements that customize Business Counterintelligence so that the CI protocols are corporate oriented. The technological perspective makes technology look like an important factor, which is a societal structure that leads to the reforming of such projections of the information society. This is stemmed from the idea of conflict innovation, which is resulted ideology since the period the Cold War started. It has extended to the business form the military form, Sputnik theory being an example of this.

The economically founded perspective is where the information is seen as a factor of the Gross National Product within the economy, and thus influencing market development for the private corporations. Because of this Business Counterintelligence data will refer to quantitative and qualitative aspects of the economic factors.

The occupationally force is where the occupational structure is patterned and analyzed as part of the informational work activities.

The spatial force is referring to the perspective of the geographical point of view and places the procedure organization on the digital map and determines an informational flow within the existing networks. There are variously disparate spatial entities that can be connected between themselves and thus confirming that the organizations is part of the information driven social organization.

The cultural perspective defines itself on the idea that the social conception has given the organization an increase of information availability within information societies. One of the advantages brought is the increase in types and channels of information available.

We have to take into consideration that the multifaceted nature of business intelligence forces the organization to structure a framework in order to maximize the results of their actions. These 5 mentioned perspectives will give companies the possibility to put into action the four functions in a

way that will maximize the protection received by them from unwanted and unauthorized access.

Cyber-crime and Business Counterintelligence

Eoghan Casey defines *Cyber-crime* as an infraction that involves a computer used in the commission of the crime, or represents the main target of this crime, and a network.[7] This notion can be divided in some subcategories:

a) Fraud and financial crimes;
b) Cyber warfare;
c) Cyber extortion;
d) Cyber terrorism;
e) Computer as a target;
f) Computer as a tool.

A resounding case of *Cybercrime* based in Russia was discovered in 2006. It references an internet site named Russian Business Network (RBN), and its administrator that shortly after its opening discover that he can earn a lot more money by hosting illegitimate activities. So he started to offer web hosting services to all kinds of criminal and objectionable activities, earning more than $150 million in one year.[8]

In recent years we have witnessed a rise in Cybercrimes and in 2017 we have had the largest cyber-attack in current history. The first was called WannaCry, started in May 12, and it cashed 52 Bitcoin ($ 130.000). At about a month later a second attack took place, Petya, it was more advanced the WannaCry, but is had an ineffective and inefficient payment system. Petya disrupted utilities like power companies, airports, public transport or central bank.

In order to stop cyber-attacks and cyber-crimes developments in the cyber-security field have advanced by in both public and private sectors. After the 9/11 attack, national agencies have registered a rise in the investigation and invest of cyber-attacks, in order to create an international infrastructure of fighting terrorism. This infrastructure consists of state organizations, private companies and universities, which develop cutting-edge research and developments. The development of the investigation capacities of the Cyber divisions is focused on the intrusions into government and private computer networks of information, destined to steal intelligence.

Because of this, Business Counterintelligence with the before mentioned functions and perspective, is oriented to determine and understand the behaviour and psychological reasoning for the attacks. Further

---

[7] Robert Moore, "Cybercrime: Investigating High-Technology Computer Crime" (Anderson Publishing, 2011), p.4
[8] The Economist, http://www.economist.com/node/9723768 accessed 29 august 2017

in the paper we will describe the Business Counterintelligence in case studies from different countries from around the world.

Case study – manifestations of Business Counterintelligence around the world

In this part of our work we will try to present some examples of *Business Counterintelligence manifestations*, and how are they used by "Big Powers" to influence the international politics.

Firstly, we will speak about Russia, one of the biggest powers until 1990, and an important actor on the international political scene nowadays. Russia has two main companies that are used to change or to blackmail other countries decisions. Even president Vladimir Putin noted that "these companies are very real and each year are accumulating more and more wealth and international influence, which they are using to advance the interests of the Russian state."[9] I think most of you already know that we will talk about "Gazprom" and "Rosneft".

Gazprom is considered an important "weapon of diplomacy" used by Russia because of its importance on the international arena. In the early 1990s, after the fall of the Soviet Union, Russian administration decided to privatize the previously state-owned businesses for being able to create a free-market economic system. This company was an exception, because the Ministry of the Gas became now a corporation named Gazprom, where the state owned more than 50% of actions.

President Putin talked in his work "Mineral and Raw Materials Resources and the Development Strategy for the Russian Economy." about the importance of this new company, and after 1999, Russian started to hire former secret and special services agents as high ranked workers in Gazprom. Even more, some oligarchs and State Duma members suspected than the corporation will be favoured by the president and his administration who wanted to monopolize the energetic sphere. Years later these suspicions have come true when "Yukos" that once was the world's largest nonstate oil company was completely dismantled, or when Shell lost its controlling stake over Sakhalin 2 project through highly questionable methods.[10]

Another "favour" is made after 2006 when the Russian state changes the rules in favour of big companies and gives them full control over their territory and the possibility to equip their "army" with firearms and UAV's produced in Russia or Israel for being able to prevent sabotage, hijacks,

---

[9] Marshall I. Goldman, Petrostate: Putin, Power, and the New Russia (United Kingdom: Oxford University Press, 2008), p.3

[10] Cindy Hurst, The Militarization of Gazprom, September - October 2010, p61, accessed 28 August 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA529212

hostage situations etc. Gazprom security service was employing more than 20000 men, who were responsible for body-guarding, intelligence and counterintelligence, plant protection, and transport of valuables, and were paid with a salary that was five or six times bigger than a security state worker salary. During the years, Russia used Gazprom to blackmail the European countries or ex-soviet states to maintain their regional influence. The most used method by Gazprom is the price raising or cutting the natural gas supply.

Such cases where reported in 2004 when Russia stopped the gas that was passing through the "Drujba" pipe to Latvia. This action was taken to encourage the privatization of Latvian companies that imported petroleum by the Russian oligarchs. Also in 2006 they stopped the gas going to Ukraine because of its "debts", or they threatened Georgia to halt supplies if they will not accept the new gas price that was 2 times bigger than the old one, and also bigger than the price proposed for other states. Of course we should not forget about its intermediaries that are more than 50 in the whole Europe, and are used to serve their own interests. Such a cases were present when Gerhard Schröder an ex-German canceler was named as Gazprom CEO, after he signed an agreement with this company that raised the Germany dependence on Russian gas, or when a audio recording between the polish oligarch Marek Dochnal and the Russian agent Vladimir Alganov where they were discussing about the privatization of the polish energy industry.

In conclusion, starting from the general definition of *Business Counter Intelligence*, we can observe that Russian officials with the Gazprom administration have undertaken a series of security measures to protect their sensitive information and interests from unwanted intruders that can harm them or their state and can alleviate their influence in the international scene.

Rosneft has a little different story. It is a company that always managed to have important contracts with foreign partners such as ExxonMobil who wanted to participate at the petroleum extraction in Siberia, or British Petroleum who signed a $1.5 billion contract for the import of 12 million tons of petroleum products.[11] Here we have a direct favoring attitude from the Russian state, or its administration, with Andrei Patrushev the son of Nicolai Patrushev (former FSB chief and Security Council) and their CEO Igor Sechin, an ex-secret agent are used to "swallow" their competitors by starting criminal proceedings against them. A good example is the case with Vladimir Evtushenko, the CEO of "Bashneft" who was forced to yield his company,

[11] *Adrian Stoica, "CONTRACTE DE MILIARDE DE DOLARI: Apetitul pentru hidrocarburile rusesti si sanctiunile economice", accessed 29.09.2017, http://www.petroleumreview.ro/ro/29-iulie-augusr-2014/190-contracte-de-miliarde-de-dolari-apetitul-pentru-hidrocarburile-rusesti-si-sanctiunile-economice*

losing $7.2 billion. After this he will be forced to pay $2.3 dollars this amount exceeding his wealth. [12]

Another proof for how important is Rosneft for president Putin is the case with the privatization of 19.5% of the company. Officially, these actions were bought by Qatar, Glencore and the Italian bank Intesa Sanpaolo, making abstraction from the EU sanctions. Analysts say that this was a political move, to show the world that even with the EU sanctions, there are countries who trust Russia and believe in its stability. After some investigations it turned out that the real buyers were not Qatar, Glencore or Intesa Sanpaolo. The only thing that is known is that money and actions passed through some phantom companies from Cayman and Singapore, but nobody is ready to offer more details.[13]

Now, speaking about the western part of the world, we will analyse Royal Dutch Shell and ExxonMobil, two very important oil and gas companies.

First of all, we mentioned the case about Shell and Sakhalin 2, a project that includes development of the Piltun-Astokhskoye oil field and the Lunskoye natural gas field offshore Sakhalin Island in the Okhotsk Sea, and associated infrastructure onshore.[14] In that period, the company was indirectly forced to sell its part of actions to Gazprom. Despite of these, in 2015 Shell started new negotiations with Russia for new projects that will cost more than $11 billion, even if Russia had a list of sanctions imposed by Europe and USA. Making abstraction from the fact that both of them will make a lot of money from this contracts, Royal Dutch Shell can be viewed as an instrument used to "control" in some limits to monitor the activity of Gazprom, their real plans and the way they work.

ExxonMobil, which is considered the largest of the world's Big Oil companies[15] always was in good relations with Rosneft because of their common profitable activities. An example can be their agreement signed in 2011 when Exxon was allowed to conduct offshore exploration in the Black

---

[12] Catalin Apostoiu, "De ce Rosneft, cea mai mare companie petrolieră a Rusiei, câştigă mereu", accessed 29.09.2017, http://www.zf.ro/business-international/de-ce-rosneft-cea-mai-mare-companie-petroliera-a-rusiei-castiga-mereu-16707949

[13] Bogdan Cojocaru, "Privatizarea Rosneft, promovată de Moscova ca un vot de încredere din partea investitorilor străini, este îngropată adânc în mister", accessed 29.09.2017, http://www.zf.ro/business-international/privatizarea-rosneft-promovata-de-moscova-ca-un-vot-de-incredere-din-partea-investitorilor-straini-este-ingropata-adanc-in-mister-16121643

[14] Miriam Elder (2008-12-27). "Russia look to control world's gas prices". Telegraph. Retrieved 2008-12-27.

[15] "FT's profile of ExxonMobil". *Financial Times*. Retrieved April 21, 2008.

Sea and the Kara Sea in Siberia.[16] There were cases when the company violated sanctions on Russia in the period when actual secretary of state Rex Tillerson was the CEO. In 2017 The Treasury Department of USA fined Exxon Mobil $2 million, which is not a significant punishment for this "mammoth".[17] Some experts consider that the good business relations between Mr. Tillerson and Mr. Sechin are responsible for this violation and were reflected in the 2016 presidential elections in USA. Now, if this was just a small part of what "business relations" can do, we can imagine what will happen in a few years.

Conclusions

Intelligence theory has shown us that it has two main sections. The first one the Business/Competitive Intelligence that is working for the company in order to find information that helps it develop. The second is Business Counter Intelligence, which protects the company from any factor that can give its competitors a development advantage over it.

As our examples showed, Business Counter Intelligence has been used by companies and states in order to protect their economic interests. Especially in the case of Russia, which is known for being a state that uses Intelligence practices in order to protect its interests, they have used may of the practices mentioned in the article in order to protect the country from any disruptive action towards the countries mineral resources. As Russia is the world leader in exporter of energy resources (crude petroleum, refined petroleum, gas and coal[18]), this has always been a sensitive matter.

Such practices are common with other countries, as the U.S.A, Peoples Republic of China, India or Germany, Russia's Government action were always visible specially with the help of the defectors that explained their tactics.

This extensive use of Business Intelligence and Counter Intelligence are widely known, but the fast moving age of information in which we live in, has made it even more relevant for a company or state to control and maximize the use of the available resources.

---

[16] Donna Borak and Matt Egan, "Trump denies Exxon permission to drill for oil in Russia", CNN Money, retrieved April 21, 2017. Accessed 05.09.2017 , http://money.cnn.com/2017/04/21/news/companies/trump-exxon-russia-sanctions/index.html

[17] Alan Rappeport, "Exxon Mobil Fined for Violating Sanctions on Russia", The New York Times, accessed 05.09.2017, https://www.nytimes.com/2017/07/20/us/politics/exxon-mobil-fined-russia-tillerson-sanctions.html

[18] http://atlas.media.mit.edu/en/profile/country/rus/

This military practice that passed into the civilian zone, has shown the development of the strategic capabilities into a powerful decision making tool. Despite the fact that Counter intelligence is a military protocol, its civilian business oriented variation has demonstrated itself as effective.

Please keep in mind that, due to the nature of Intelligence, Business Counterintelligence will always have a restrictive character from the point of view of an academic, as the detailed aspects addressing its protocols and best practices will be kept as private as possible. Keeping this in mind and thinking about the functions and forces affecting Business Counterintelligence, we can conclude that there is no specific "receipt" to put this process into action. We have saw the way in which it is performed by the Russians companies and what affects it had on their counterparts.

References:

1. Carlisle R., " Encyclopedia of Intelligence and Counterintelligence",2015, Routledge.
2. Cojocaru, Bogdan, "Privatizarea Rosneft, promovată de Moscova ca un vot de încredere din partea investitorilor străini, este îngropată adânc în mister", accessed 29.08.2017, http://www.zf.ro/business-international/privatizarea-rosneft-promovata-de-moscova-ca-un-vot-de-incredere-din-partea-investitorilor-straini-este-ingropata-adanc-in-mister-16121643
3. "Counterintelligence – Best Practices for Cleared Industry ", 2014 , accessed 20.08.2017 at: https://cyberwar.nl/d/20141028_US-DoD-Counterintelligence-Best-Practices-for-Cleared-Industry_CIBooklet.pdf
4. Elder, Miriam, (2008-12-27). "Russia look to control world's gas prices". Telegraph. Retrieved 2008-12-27.
5. Goldman, Marshall I., Petrostate: Putin, Power, and the New Russia (United Kingdom: Oxford University Press, 2008)
6. Harber, J.R., "Unconventional Spies: The Counterintelligence Threat from Non-State Actors", 2012, accessed15.08.2017 at: https://modularconstructionna. iqpc.com/media/6089/476.pdf
7. Hurst, Cindy, The Militarization of Gazprom, September - October 2010, accessed 28 August 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA529212
8. Michal K., "Business counterintelligence and the role of the U.S. intelligence community", 2008, International Journal of Intelligence and Counterintelligence Vol. 7 , Iss. 4, accessed 10.08.2017
9. Moore, Robert, "Cybercrime: Investigating High-Technology Computer Crime" (Anderson Publishing, 2011), p.4
10. "Protecting Key Assets: A corporate Counterintelligence Guide", DNI, accessed 22.08.2017 at: https://www.dni.gov/files/NCSC/documents/Regulations/ ProtectingKeyAssets_CorporateCIGuide.pdf

11. Stammberger, S., "GoogSpy: Business Counter Intelligence for Everyone", accessed 5.09.2017 at: http://www.intelligencesearch.com/ia048.html

12. Shear, C.J., "Business Counterintelligence: sustainable Practice or Passing Fad?", 2009 , accessed 15.08.2017 at: http://hdl.handle.net/10019.1/1930

13. US Marine Corps, "Counterintelligence – MCWP 2-6", 2016, accessed 22.08.2017 at: http://www.marines.mil/Portals/59/Publications/MCRP%202-10A.2%20(Formerly%20MCWP%202-6).pdf?ver=2016-06-01-135919-697