EasyChair Preprint

№ 264

Ocean's Thirteen in the port of Antwerp. Reflections on how IT specialists were rounded up by maritime cocaine smugglers.

Rafael Rondelez

June 15, 2018

Ocean's Thirteen in the port of Antwerp.

Reflections on how IT specialists were rounded up by maritime cocaine smugglers.

Lic. Rafael Rondelez, Doctoral Researcher at Ghent University (Belgium)

Abstract

Technological innovation continues to shape society and economies and - by extension - the serious and organized crime landscape in Europe as well as in other parts of the world. The fourth industrial revolution[1] will undoubtedly bear consequences for the entire spectrum of crime. Society will increasingly face complex technological crime issues while new - cyber driven - criminals will continue to appear upon the horizon.

The cybersecurity research community recently started to broaden its vision (Leukfeldt, 2017). It is now moving away from primarily discussing technological aspects towards the analysis of non-technological issues such as the human factors and other socio-technical matters related to cybersecurity and -crime. In doing so, the expectation is held high that this approach will enable society to take the step from merely discussing technological aspects of stopping cyber incidents and attacks, to understanding and preventing individuals who are involved in, or seek, to commit cybercrime or cyberterrorism.

This article aims to contribute to this objective as it discusses a recent case where so-called white or ethical hackers[2] joined forces with a traditional organized crime group and assisted the smuggling of narcotics representing a value of several tens of millions of euros. The focus of the paper is not so much on the technological aspects of this cooperation but on exploring the social dynamics which led these guys to experience their worst nightmare.

***Keywords**: organized crime, cocaine smuggling, cybercrime, cybersecurity, social dynamics, human factors.*

1 Introduction

Smuggling has been and still is one of the most common economic activities of all time. While this forbidden economy involves the contraband of commodities, it also concerns the trafficking of fear-inducing things such as narcotics, weapons and human beings.

Besides the motives, it can be argued that two basic conditions are decisive for the nature and extent of smuggling activities: human cooperation and technology. In fact, individuals are - for as long as humans are humans - involved in cooperative trading including reaching out to distant peoples. In addition, the scope of trading opportunities has always been and still is largely determined or influenced by technological possibilities. This is also the case for organized criminal groups, irrespective whether organized crime (OC) is defined as a one-dimensional or as a multi-dimensional concept.

Whilst organized criminals take advantage of the ubiquitous available information and communication technologies to develop more networked or cellular structural co-operation, they increasingly explore new digital ways to consolidate and expand impersonal drug smuggling operations. The latter has recently been demonstrated in the port of Antwerp (Belgium) as several Flemish IT-specialists hacked the networks of shipping companies and container terminals and provided transnational drug traffickers with the necessary information to steal containers loaded with cocaine or heroin from the harbor premises.

The growing interconnectedness between international drug trafficking and cybercrime on the one hand and the evolution towards more networked criminal cooperation on the other hand, raised a sense of urgency amongst shipping companies, security actors and policy makers in Antwerp. Shipping companies and the port

[1] The fourth industrial revolution refers to the advent of "cyber-physical systems" and signifies the fusion of technologies which blurs the lines between the physical, digital and biological spheres.

[2] In Internet slang 'white hat' or 'ethical' hacker refers to a computer security expert who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems. The hacking is authorized by or performed by a company or an individual to help identify potential threats on a computer or a network. The opposite of 'white hat' is a 'black hat' hacker who unauthorised violates computer security for maliciousness or for gain (Goodman, 2015).

authorities decided to gradually automate the container release processes by introducing cryptography - often commonly referred to as blockchain technology - to squeeze out any human interaction in the generation and transmission of PIN codes. Subsequently, local as well as national politicians declared the 'war on drugs' in the port of Antwerp[3] and recently presented a comprehensive action plan[4]. The central objective of this initiative is the creation of a nodal and multi-disciplinary task force of approx. 80 representatives from the police, tax authorities, customs, social inspection and the public prosecutor's office.

However, these initiatives are based on implicit assumptions about traditional mobsters and their criminal behavior while the human factor in cybercrime is largely overlooked. As such, the question remains whether cybercriminals are to be considered as new types of offenders or whether they remain traditional criminals on new turf? In fact, there remains little criminological research regarding the patterns and factors contributing to the entry into cybercrime, continuity, and desistance, linking specifically with the role of transnational organized crime. Hence, more theoretical as well as empirical research is needed to better map the various trajectories and factors of cybercriminals to develop and complement more effective and efficient policies and security agendas.

To bridge this knowledge gap, this article analyses the story of three Flemish IT specialists who became the main characters in the so-called Ocean's Thirteen case[5] in the port of Antwerp with the objective to identify particularities in their personality, course of life, criminal motivations and social networks. In doing so, it is envisaged that the analysis will allow to better grasp potential interconnectedness between traditional organized crime groups and cybercriminals. In addition, this contribution also envisages to provide insights and points of attention for the various actors who will play a role in the digitization of the port activities and in the implementation of the proposed plan. At the same time, this contribution also represents a plea for more scientific research regarding the human factors of cybercrime.

This analysis is the result of the application of qualitative research methods: a case study complimented with semi-structured interviews. The case study concerns the analysis of open source information - press articles[6] - related to the story. Additional insights were obtained from various domestic and international experts in the maritime, cybersecurity and related financial sector[7]. Semi-structured interviews were held on site or through voice and video phone calls over the internet. In addition, information was also collected through e-mail correspondence.

The paper is structured in five parts. Following the introduction, conceptual clarity is provided regarding the technologies used in smuggling cocaine through the port of Antwerp. This part is followed by a detailed reconstruction of the Antwerp Ocean's Thirteen case. Section four reports about an *ex post* analysis of the social dynamics between the IT specialists which ultimately led them to become the masterminds of a hacking operation for one of the biggest drug-smuggling operations in Europe. Conclusions and recommendations are presented in the final part.

2 Maritime cocaine smuggling technologies: some concepts.

Before delving deeper into the human factors that bring about the growing interconnectedness between organized crime groups and cybercriminals, we will first bring some conceptual clarity into technologies used in narcotics trafficking through the port of Antwerp.

[3] Antwerp operates as one of the main entry points for cocaine from South America. In 2015, nearly a quarter of the total amount of seized cocaine in the European Union was discovered in the port of Antwerp. Last year, the total amount of maritime cocaine seized in the port topped nearly 40 metric tons (Huybrechts, 2018).
[4] This plan - called 'Stroomplan tegen drugscriminaliteit' ('flow plan against drugs crime') - was presented to the press on 21 January 2018.
[5] Ocean's Thirteen refers to the 2007 film directed by Steven Soderbergh. The plot of this film is about a group of criminals led by Danny Ocean which plans to rig the slot machines of one of Las Vegas casinos. However, to succeed, the group must disrupt a state-of-the-art computer system - called 'Greco' - that 'continuously monitors the gamblers' biometric responses and predicts when cheating is occurring.
[6] The analysis is principally based on articles retrieved from the following websites: Motherboard (2013), Bloomberg (2015), Crimesite (2013; 2015), Het Laatste Nieuws (2017) and De Tijd (2017).
[7] All respondents were granted anonymity.

The different technologies are regularly defined in an abstract way, which often leads to a 'Babylonian speech confusion'. It is therefore important to highlight those concepts which are significant for the context of this publication.

At the low-tech end of the drugs smuggling continuum is the technology known as 'ripping off'. Upon arrival of the ship in the port of Antwerp, criminals are eager to get hold of their cocaine shipment as quickly as possible and without anyone noticing it. A classical rip off only lasts a few minutes as low volumes of cocaine are usually packed in sports bags which are concealed within a container.

While there are several ways to organize a rip-off the most basic forms are executed by the traffickers themselves or by 'runners'. In addition, organized crime groups regularly bribe dock workers with 'quick' and 'easy' money in return for 'lending a hand' by moving containers to a safer place within the harbor area[8]. Traffickers either cut the fence and steal the cocaine from the container themselves or they rely on 'runners' to bring the cocaine to a place nearby a fence, so they can pick it up easily and unnoticed.

This technique became significant over the last years according to the EMCDDA. While only 32 % of the seized cocaine followed the use of the 'rip-off' technique in 2010, the number had doubled by 2012 to 70 % (European Monitoring Centre for Drugs and Drug Addiction and Europol, 2016).

While the 'ripping off' technique is perfect for taking possession of low volumes, it is not suitable for unloading more voluminous cocaine shipments in the harbor. Hence, organized criminals favor a more elegant and less risky way by stealing pin codes as they try to fool the electronic container release procedure.

Containers, when discharged from ocean carriers, are temporarily stored in a container terminal until they are released by the shipping company. Upon paying the shipping costs by the forwarder, the shipping companies generate pin codes which they forward to the container terminal and the forwarder.

The forwarder normally sends the pin codes to the transport company charged with picking up containers at the terminal. The final security verification happens at the container terminal when the transporter enters the pin code into a keypad.

However, the system fails due to the human interaction in the transmission of the pin codes. While the pin codes are generated electronically, the transmission to the forwarder and container terminal is not automated. Pin codes appear upon computer screens and are communicated either by e-mail or by phone. Consequently, as transport companies regularly outsource orders to sub-contractors, they pass the pin codes verbally on to the drivers who write them down on a piece of paper. This paper is then presented at the entry of the container terminal and the sub-contracting transporter can pull out a container from the terminal.

Criminals are very eager to intercept the pin codes as it allows them to steal containers before the legitimate transporter arrives at the terminal entry port. While organized criminals still rely on traditional methods to obtain information (such as burglary or bribery), there is evidence that they are also increasingly experimenting with information and communication technologies. The latter, of course, blurs the line between traditional OC and cybercrime.

Cybercrime is however too generic as definition as it serves as an umbrella concept (McGuire & Dowling, 2013). Cyberattacks can be classified within two main categories depending on the type of technology applied: cyber-enabled[9] or cyber-dependent crimes[10]. To complicate matters even more, there is a third category which is gaining importance: cyber-hybrid crimes. The latter represents criminal activity characterized by a combination of both cyber-enabled and cyber-dependent crime techniques.

The third category is often committed when traditional OC methods or cyber-enabled techniques do not yield the expected information or results. It is in this phase that 'old school' organized criminals turn to IT specialists to help them out. The latter is demonstrated in the following section as we outline a recent case[11] - referred to

[8] The bribes are quite substantial. Bloomberg (2015) - for example - estimates that they amount to 10.000 euro a 'trip'.

[9] Cyber-enabled crimes are 'traditional' crimes which do not necessarily require the use of computers, computer networks and information or communication technologies (ICTs). However, the application these ICTs helps to increase the scale or reach of these crimes.

[10] Cyber-dependent crime or 'pure' cybercrimes are offences that can only be committed by using a computer, computer networks or other forms of information and communication technology.

[11] The investigation lasted from fall 2011 till the summer of 2017. The case was introduced before the Court of Antwerp at the beginning of December 2017, however until today no final judgement has been reached.

as ‘Antwerp Ocean’s Thirteen’ - on how Dutch/Turkish organized criminals hired Flemish IT specialists - so called ‘ethical hackers’ - to develop high-tech data interception devices necessary to consolidate and expand their drugs smuggling activities through the port of Antwerp.

3 From mangoes to ‘pwnies’.

The beginning of this plot is situated in 2011 when a criminal organization headed by a Dutch national - Frits Becker - is very active in ripping off narcotics - primarily South-American cocaine - from containers. The modus operandus consist of transporting illicitly obtained containers from the port of Antwerp to safe warehouses in The Netherlands where drugs shipments can be easily ripped off.

They rely on a separated group of dedicated drivers to collect the containers in the various terminals in Antwerp. In addition, they also rely on Turkish nationals - Orhan Adibelli and Ahmet Okul - to provide them the pin codes which the drivers need to access the container terminals and pick up the concerned containers prior to the arrival of the legitimate transport company.

Adibelli runs a dodgy fruit (mangoes) import-export company in Barendrecht (The Netherlands). He is very close with Ahmet Okul who owns a store in Arnhem (The Netherlands) and sells bugging devices. While they are both into technology - Okul is very interested in the art of hacking - can Adibelli be regarded as the financial guy, the one with the money.

The ‘dirty work’ - obtaining pin codes from shipping companies - is Okul’s job as he has more advanced knowledge and skills in ‘spying’. Initially he applies cyber-enabled techniques such as phishing e-mails but gradually moves on to more cyber-dependent crimes. He bombards shipping companies with malware which he sends by e-mail. However, as many of Okul’s messages fail, both men are in search of new ways to harvest valuable pin codes. They are desperately seeking someone who can help them in manipulating global logistical and transportation networks to intercept and capture network traffic.

In the same period, the Flemish IT specialist and ethical hacker Filip Maertens is working on the expansion of his smartphone data mining startup 'Argus Labs'[12]. He is looking for investors who are prepared to provide him with the necessary capital: more than 1 million euros.

By chance, Filip Maertens meets Orhan Adibelli, a potential investor. The latter is currently constructing a new office and Maertens offers him - as token of his entrepreneurial skills - help. He advises Adibelli on the purchase and installation of computer equipment.

Despite a good relationship and trust between the two men, Adibelli decides to break the deal in December 2011. However, prior to his decision, he introduces Maertens to his associate Ahmet Okul. The latter immediately shows his unrestrained interest in the knowledge and skills of Maertens concerning penetration testing[13] and 'pwnie' devices[14].

The reason why Adibelli called off the deal is unclear, but possibly originates in the seizure of signal-jamming devices, keylogging software and IMSI-catchers[15] by the police during a search in his flat in Rotterdam in autumn 2011. In addition, the officers had found traces of his involvement in maritime Europe-bound cocaine smuggling from South America. They had also discovered information about Maertens’ security company

[12] Argus Labs developed the 'Jini' platform which analyzes data from sensors in smartphones with the aim of providing the user of a smartphone, personal advice and feedback (for example when it's time to leave for a meeting considering the expected amount of - little or much - traffic on the road).

[13] Also referred to as pen testing, is an authorized simulated attack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses or vulnerabilities, including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

[14] ‘Pwn’ is hacker slang meaning ‘to compromise’ or to ‘control’ based on the previous usage of the word ‘own’ (pwn is pronounced as ‘pown’). In essence, ‘pwnies’ (pronounced as ‘pownies’) refer to mini-computers disguised as power strips and internet routers which are used to intercept network data or to ‘owning someone else’s network’.

[15] An International Mobile Subscriber Identity-catcher - or IMSI-catcher - is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users. IMSI-catchers are mainly used by law enforcement or intelligence services.

'Avydian' and notes related to a meeting with Maertens where references are made to Antwerp based shipping companies.

However, hoping that Adibelli changes his mind and invests money in his 'Argus Labs', Maertens provides private lessons to Okul on hacking techniques and methodologies. It is during one of these lessons that Maertens receives the question from Okul to provide him a 'pwnie' to satisfy the needs of a client.

But Maertens refuses and one week later he is summoned into the office of Adibelli in Barendrecht where he meets, besides Adibelli and Okul, two unidentified men. On that occasion he is brutally attacked by Okul and Adibelli. In addition, they blame him for the fact that their customers - presumably the two unidentified men - are losing a lot of money due to his non-cooperative attitude.

On his way back, a distraught Maertens calls in the help from his childhood friend: Davy Van De Moere. Though their first consideration was to report everything to the police, they quickly abandon that idea as they fear for reprisals from Adibelli and the others. Hence, their decision to go mute and stop responding calls, hoping that everything will blow over. Unfortunately, a week later, Maertens again receives a call from - a friendly - Adibelli, who invites him for a new meeting in his office in Barendrecht.

Terrified of going alone, Maertens requests Van De Moere to accompany him. Maertens would attend the meeting while Van De Moere would wait in the car in the immediate vicinity of Adibelli's office. In case Maertens would have to flee, Van De Moere would be able to pick him up. However, their plan fails, Van De Moere is detected, and he is also summoned to join the meeting. In the presence of Van De Moere, Adibelli and Okul apparently speak frankly about the fact that their phishing initiatives did not produce the desired results. They ask Maertens to build a 'pwnie' on short notice.

On their way back, Maertens and Van De Moere think about their 'assignment'. As going to the police was no option, they look for a way out. In doing so, they consider that building a 'pwnie' would not make them liable of committing an offence as these devices are available through the Internet. They fell reassured in the sense that they consider themselves as merely suppliers and not as operators of the device.

Subsequently, Maertens and Van De Moere decide to call upon the assistance of another childhood friend: Wence van der M[16]. Together they develop a device which looks like a European power strip which entails a tiny Linux computer running a powerful hacking software called 'Metasploit'. The pwnie can transmit data via cellular networks, meaning that they can access it remotely using a 3G connection[17].

However, a couple weeks after delivery of this pwnie Maertens and Van De Moere are again summoned to Barendrecht. There they are told that their pwnie did not work and are intimidated by Adibelli who threatens them with a handgun. In the meantime, reference is made to a recent murder in the Rotterdam crime scene. Finally, a sum of 25.000 euro is thrown in their hands with the caution that this would motivate them to make the pwnie work.

At that time, as they realize that they have no way to escape, Maertens and Van De Moere devise an ambitious plot of their own, hoping to dodge the mobsters and police alike. In fact, the pair decides to bluff by reconfiguring or making small sabotages. As such, they pretend that they are cooperating but apparently fail to deliver a proper functioning device. In fact, they hope that the mobsters will finally give up and stop the cooperation. During several months they develop and deliver various deficient pwnies.

However, the sabotage plan does not work out. By June 2012 they are told to meet two men in a bar in the harbor area in Antwerp and to hand over an improved pwnie. These men seemed to be the ones responsible for breaking into the shipping companies and installing the pwnies. Okul insists that Van De Moere explains in detail how the men must handle the pwnies.

In July 2012, Van De Moere and Maertens are again instructed to meet Okul in the same bar in Antwerp. Van De Moere initially refuses but soon changes his mind when the caller starts to recite the addresses of his family members as well as his private address. During the meeting Okul intimidates the couple and forces them to follow him to Barendrecht where Adibelli is waiting to meet them.

Van De Moere is, upon their arrival in Barendrecht, instantly threatened by Adibelli and receives a new assignment. Van De Moere must drive to specific office buildings to check whether the implanted pwnies are working properly. To execute this job, he receives two antennas from Okul.

---

[16] His family name is not mentioned in any of the examined press articles.

[17] 3G, short for third generation, refers to the third generation of wireless mobile telecommunications technology.

Mid-August 2012, Van De Moere parks his personal Subaru with open hood near the offices of DP World - a Dubai-based port operator - in Antwerp. He connects one of the antennas to the battery of his car and he starts skimming the secret network of the company. However, his attempt to obtain pin codes fails.

In fact, a few days earlier - on 15 August - members of the criminal group had penetrated the offices of DP World and installed small USB devices onto the company's computers which were programmed to intercept the nine-digit PINs that controlled access to the company's shipping containers. However, the burglary did not go unnoticed and the police was called. During their investigation at DP World it appeared that similar data interception devices had been installed in other companies in the harbor of Antwerp. As such, it was established that a bunch of similar surveillance devices were detected in the offices of Mediterranean Shipping (MSC), a large Swiss shipping company. Upon request of the police, MSC confirmed that its container-tracking systems had been breached. MSC also told the police that they had instructed PriceWaterhouseCoopers (PwC)[18] to conduct an internal investigation and to secure their network.

Wence van der M. - who took part in Maertens and Van De Moere's conspiracy - heads the PwC investigation but finds himself in a compromising position. His team needs to analyze a pwnie which he helped to develop. But, he remains silent and the PwC investigation team submits its report. According to PwC, computer hackers had intercepted MSC's network traffic, potentially in view of obtaining pin codes and hijacking MSC's containers.

In addition, police investigators discovered on 17 August 2012 a pwnie device in the offices of the Chilean shipping company CSAV in the London Tower in Antwerp. Apparently, this device had already been installed at MSC in June 2012. The location of detection - the London Tower - was however not a coincidence as Maertens, accompanied by Van de Moere and Adibelli, had visited the tower on 9 November 2011 in search of office space for his companies Argus Labs and Avidyan. Whilst visiting the location, Van de Moere was requested by Maertens to check the networks within the building.

During the DP World investigation, the police analyzed CCTV footage of the parking lot and saw a man behaving strangely whilst an antenna is connected to the battery of his Subaru.

By the fall 2012, Maertens and Van De Moere, find themselves with little to do. The most plausible explanation is that the pin code operation had been exposed and port companies had removed the hacking tools from their networks. In September 2012, Adibelli summons them to Barendrecht for another meeting.

Whilst Maertens and Van De Moere fear for the worst, Adibelli asks them if they want to quit. Both say yes and Adibelli agrees. However, there is one condition for their release: Van De Moere must give Okul an intensive training session on Linux - the operating system on which the hacking software Metasploit - is based. A few weeks later Van de Moere provides the training during a weekend at a Holiday Inn in Ghent (Belgium). That is last time he saw the Turks.

On 11 June 2013, a joint Dutch and Belgian police operation took place. Various house searches are carried out simultaneously in The Netherlands as well as in Belgium. Adibelli and Okul are however not arrested as they had fled to Turkey. The Belgian police arrests Van De Moere at his house. Maertens is abroad as he is spending some time in Southern France but immediately returns to Belgium when he receives word of the arrest of his friend. He presents himself to the police the next day. Van der M. is also arrested, however a few weeks later.

Members of the organized crime group are charged by the Dutch and the Belgian public prosecution office for various criminal acts including suspicion of drugs smuggling and membership of a criminal organization. Van de Moere, Maertens and Wence Van der M. appeared before the Court in Belgium at the beginning of December 2017 (Lefelon, 2017). Besides being accused of hacking, they also face charges of conspiracy to smuggle drugs and involvement in a criminal organization. They are considered to be jointly responsible for illegally intercepting information (pin codes) which facilitated members of a criminal organization to steal 16 containers concealing high quantities of narcotics from the harbor premises in Antwerp in June 2012. It is suggested that their technical support allowed the criminal organization to smuggle 3 metric tons of cocaine and 1 metric ton of heroin, representing a value of several tens of millions of euros.

It is now waiting what the final verdict will be from the Belgian Court.

4 Brothers in arms.

[18] PwC is one of the Big Four auditors with headquarters in London (UK). The other three big accounting and consulting companies are: Ernst & Young (EY), KPMG and Deloitte.

It is tempting to call this example a typical case of general strain (Agnew, 2001). Following this theory Maertens' motivation to engage in a criminal adventure, involving his fellow friends, originates in the fact that he became distressed when Adibelli broke up the deal. The fact that Maertens would otherwise fail to achieve his objective - the long-expected investment - made him to join forces with organized criminals.

While this theory may clarify some of Maertens' behavior, it certainly fails to explain the behavior of Van De Moere and W. Van der M. As such, the mystery remains why a group of friends from the upper world turned into 'black hat' hackers.

To lift this veil, we conducted an *ex post* analysis of the social dynamics of the group. The justification for this approach originates in the assumption that the behavior of this group is mainly determined by the interactions of the individual group members and not by ethnic or other social and socio-economic circumstances.

In the next paragraphs, we outline demographic and socio-economic statuses together with an analysis of other related subjects such as social learning, IT knowledge, routine activities, subculture and criminal career.

Based on the demographics, it appears that the analysis concerns activities of three young men in their early thirties (Filip Maertens and Van De Moere are both born in 1978 whilst Wence Van der M. was born in 1972) with a Flemish ethnic background.

From a socio-economic perspective, there is no doubt that Maertens, Van De Moere and W. Van der M. did very well in society back in 2011. At that time, Maertens and Van De Moere are considered by various media as the 'wonder boys' of the Flemish IT sector. Wence van der M. is referred to as one of Belgium's most qualified 'penetration testers'.

In 2011 Maertens - already married - earns 20.000 euro a month as an independent consultant. He runs his own company - called Avydian - based in Tielt (Belgium) and provides cyber security advice. He is - for example - involved in the development of mobile channels for Fortune 500 banks. In addition, he is the president of the cyber security commission within the Belgian based European Corporate Security Association (ECSA)[19] where he expands his network with top people from public and private security services. Van De Moere earns at that time 12.000 euro a month as chief technology officer of Mondial Telecom, a Belgian mobile software company. Wence Van der M. joins PwC in July 2011 as manager/team leader 'cybersecurity' and receives a personal security clearance from the Belgian National Security Authority[20].

Maertens and Van De Moere, credited for their IT-skills, are regularly solicited by Belgian journalists to provide comments on hacking matters. Their high potential is also noticed by Ernst & Young - one of the four major auditing companies - as the company often temporarily hires them to perform computer audits.

Maertens, Van de Moere and Van der M. demonstrate their abilities to successfully follow - often - intensive and high level technical education and training programs. Filip Maertens graduates a BSc in Experimental Psychology (Katholieke Universiteit Leuven) and obtains a MSc degree in Information Security at the Eindhoven University of Technology. Van De Moere succeeds his studies at the Europese Hogeschool Brussel (EHSAL) while Wence van der M. obtains a bachelor's degree in applied computer science, specialization networking at the Erasmushogeschool Brussel. The latter additionally attends the Young Management Program at the Vlerick Business School.

Consequently, it is genuine to esteem that these young men are intelligent and possess the necessary self-control to plan and manage their businesses. In addition, both - Maertens and Van De Moere - display to be very driven and ambitious. In 2008 Van De Moere creates his startup 'Attractel' whilst Maertens is completely captivated in 2011 by the launch of his startup 'Argus Labs'.

Regarding the topic of a criminal career, it is obvious that Maertens, Van De Moere and Wence Van der M. did not have a career in such terms as they did not have a criminal record back in 2011. However, when rephrasing the subject into deviant careers, the analysis reveals indications in the personalities of both Maertens and Van De Moere of moving on the edge of deviant behavior and morality.

Since the start of their friendship - at the age of 14 - the relationship is dominated by a common passion for hacking or activities which are legally contested and (still) are considered a crime. In fact, their first encounter

[19] The mission of ECSA is to serve as an association of professionals from the public, private and academic sector who are active in, or contribute to the security, the continuity or the resilience of corporations, organizations and institutions (www.ecsa-eu.org).

[20] The National Security Authority provides - under certain conditions - security clearances for employees of public and private entities to control access to classified information (https://www.nvoans.be/nl).

originates in a dispute regarding the hacking of Maertens' bulletin board - called 'Bad Habbit' - by Van De Moere. The initial 'click' between the two-young men is gradually strengthened and deepened each time they meet. During their regular meetings they discuss computers or exchange books about programming.

At the age of eighteen they are among the pioneers of the Belgian hacking scene. They develop and govern an internet relay chat (IRC) forum called 'Securax'. The latter is the digital meeting place for members of the Belgian hacker community. At the top of Securax there are about 100,000 subscribers.

Besides their boundless passion for hacking they also display signs of unethical morale as they seem to have no shame to deceive people. The latter is illustrated by the fact that Maertens - when he was double-booked for meetings - relied on Van De Moere to provide presentations whilst pretending to be Maertens. The latter also played his card of deception in trying to fool Adibelli and Okul by shaving his head, pretending he had been diagnosed with a brain tumor. In doing so, he hoped he would get away and escape from their claws. Unfortunately, neither Adibelli nor Okul bought his trick. The tendency to deception returns when Maertens and Van De Moere developed their plan to construct ill working pwnies. As such, they wanted to deceive the mobsters as well as the police. References to Maertens' deception capabilities are also made by Van De Moere as well as Wence Van der M. when they are arrested and interviewed. Both blame Maertens for misleading them.

During the analysis no indications were retrieved regarding a potential early deviant career of Van der M., however he must have felt similar impulses for the subject of hacking, at least for the world of 'white' hackers, when considering his later studies and training.

Maertens, Van De Moere and W. Van der M. consider themselves as 'ethical hackers'. They obtain their initial IT knowledge through self-study and later they also receive more specific training either at school or through the respective academic trainings. However, there are also indications which reminds us of Sutherlands' differential association theory (Gaylord & Galliher, 1987). There is no doubt that they - Maertens and Van De Moere - developed their hacking skills through social learning and mutually influenced each other in this domain. But, there are also reasons to believe that both must have met - known or unknown - peers. Their IRC Securax provided the ideal medium for social learning and contacts with like-minded individuals.

Furthermore, the analysis did not provide any indication that their behavior displeased one another, on the contrary, they made a profession out of their 'hobby'. Thus, their routine activities - advising people and businesses on cyber security or cybercrime - constantly offer them opportunities to delve deeper into their passion. In other words, their lives consist merely of nothing else but 'hacking'.

Based on the analysis, we argue that Maertens and Van De Moere developed a subculture which allowed them to consider their acts - their co-operation with organized criminals - as normal, at least, as not being criminal. We illustrate our account by referring to the fact that - when Maertens and Van De Moere are summoned to produce a pwnie - they do not regard themselves as criminals or as being involved in criminal activities. In fact, they rationalize and neutralize (Sykes & Matza, 1957). For them, developing a pwnie does not turn them into criminals. On the contrary, they blame the others as being criminals. In fact, are Adibelli, Okul and the unidentified men not the ones who install and operate the pwnies to capture network traffic data?

The latter is quite remarkable and even frightening as it appears that two of the best trained Belgian IT specialists - ethical hackers - do not know that developing a hacking tool is considered a crime under the Belgian penal code[21].

In this section, we discussed the result of the analysis of the social dynamics between Maertens, Van De Moere and W. Van der W.

Based on the results, we claim that Maertens and Van De Moere are to be considered as Siamese twins. Their fusion process dates back to the day they met. And although they are not physically connected, they are bound by their strong mental bond. Their inexhaustible passion for hacking serves as a source from which they evolved into brothers in arms. As can be expected from close associates, they fight together on the same side in times of trouble such as intimidation, violence and life-threatening threats.

This bond unquestionably determines the behavior of both Maertens and Van De Moere. When Maertens gets into trouble, he knows he can unconditionally rely on the help and support of Van De Moere. Van De Moere blindly trusts his soul mate and asks few or no questions. In addition, they jointly neutralize any thought which

[21] The possession, development, sale, reception in view of use, import or dissemination of hacking tools are punishable following the provisions of article 550bis of the Belgian penal code (Kerkhofs & Van Linthout, 2013).

could undermine the execution of their intentions. They do not consider their actions as intrinsic criminal or wrong, on the contrary they blame the others.

From this perspective, the choice of Wence Van der M. to join Maertens and Van Der Moere can be justified. Maertens and Van de Moere are his friends and he trusts them blindly. Overall, they are - just like him - successful and respected - ethical - experts in hacking so why should he doubt or ask critical questions about their intentions or activities.

As such we feel confident when arguing that the Antwerp Ocean's Thirteen case clearly demonstrate that social dynamics between individual ethnic 'hackers' can transform these individuals into a group or an association of 'black hat' hackers willing – at least neutralizing every moral obstacle - to support the activities of an organized crime group.

5 Conclusion and recommendations

Cybercrime and the threat of computer-related attacks are growing daily, and the need for security professionals who understand how attackers compromise networks is growing right along with the threat. Subsequently, government agencies and private companies rely on "ethical hackers" or professional security testers to put their networks to the test and discover vulnerabilities before attackers do.

It is to be expected that 'ethical hackers' will assume an increasing role and position in the ecosystem of cyber security and the fight against cybercrime. After all, following the pressure from the fourth technological revolution, our society will continue to digitize and roboticize. The developments concerning the Internet of Things, artificial intelligence, encryption (for example blockchain technology) and machine learning mean that evolution will not only be limited to general socio-economic life, but that the technology will also influence our physical and psychic life more radically.

While the interest in the immensely rapidly developing technological domain - without doubt a fascinating world - is increasing, the awareness about the human factors of cybercrime remains low. Or, in other words, what do we know about the individual behind hacking? Do we study him / her enough?

The latter is a legitimate question as at this moment much academic interest goes to the study of information and communication technologies (ICTs). Perhaps this choice follows the prioritization of solving the technical issue on how to stop cyber incidents and attacks. However, understanding and preventing individuals or groups of becoming involved in the planning, preparing and execution of cybercrime (including cyber terrorism and espionage) is equally important. The case study related to the activities of IT specialists in facilitating narcotics through the port of Antwerp clearly demonstrates this and underlines the urgency to turn the stern and set sail for more academic research of the human behind the (ethical) hackers. The case study shows that we currently do not have a ready-made answer to the question whether hackers are now a new type of criminal or whether they are traditional offenders on new turf.

Although there is a danger in drawing conclusions from a single case study, the study nevertheless illustrates several critical issues.

The first issue relates to the way guidance is provided to high-potentials who want to invest in the world of startups. These individuals are enormously eager to obtain money as the latter is often their only life-line between failure and success. Consequently, this makes them extremely vulnerable for criminal exploitation. They are only focused on dollar or euro signs in the eyes of so-called investors which make them loose every connection with reality. The latter is very well illustrated by Filip Maertens.

As a recommendation I would suggest to provide better guidance and information for people who want to launch a startup. The danger of exploitation of their technological knowledge in exchange for participation in traditional or cybercrime exists as was demonstrated.

Another issue relates to support and guidance of 'ethical hackers'. Ethical hackers in Belgium - and perhaps also in other countries - are often pushed in the twilight zone as their core business - hacking or penetration testing - is fundamentally prohibited by law.

The ethical nature of their actions is determined and depends on a contract between the 'hacker' and the company that appoints or hires the 'hacker' to test or check the network for any security breaches or defects.

In Belgium, there is no legal framework that - unambiguously and clearly - describes the position or role of an ethical hacker. The Cyber Crime Center of Belgium has recently developed a 'responsible disclosure' formula that companies can post on their website and where they indicate that hackers can test their systems on

condition that they report any vulnerability they encounter to the company. This is the framework in which ethical hackers can work according to this explicit guideline. However, the question is whether this framework is sufficient, as the responsible disclosure fails to satisfy security researchers who are expected to be financially compensated as the latter might be viewed as extortion.

It is therefore advisable to officialize the profession of 'ethical hacker' and to draw up a professional code for this category. This would at least allow to enter a dialogue between government officials and the ethical hacker community and as such remove the veil of secrecy surrounding the individual of an 'ethical hacker'. Regular consultation would also provide the means to better outline - for example - the penal provisions regarding hacking and thoroughly explain potential consequences of cybercrime. It was striking to establish during the analysis that neither Maertens nor Van De Moere were aware of the penal code and did not have any confidence in the police even though Maertens had several high-ranking police representatives in his network.

Finally, we plea for more academic research regarding the human factors related to cybercrime. The Antwerp Ocean's Thirteen case shows that even a single case study yields interesting background information regarding the social dynamics of cyber criminals. Consequently, profound analysis might provide more insight into their actions, which would offer better perspectives for more effective and efficient prevention and combating of cybercrime.

References

AGNEW, R. (2001). Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency. *Journal of Research in Crime and Delinquency*, 38(4), pp.319-361.

Crimesite. (2013). *Tech-ondernemers in cokezaak - Crimesite*. [online] Available at: https://www.crimesite.nl/tech-ondernemers-in-cokezaak/ [Accessed 26 Mar. 2018].

Crimesite. (2015). *Gehackte haven, cokesmokkel 2.0 (#1-6) - Crimesite*. [online] Available at: https://www.crimesite.nl/gehackte-haven-cokesmokkel-2-0-1/ [Accessed 26 Mar. 2018].

European Monitoring Centre for Drugs and Drug Addiction and Europol (2016). *EU Drug Markets Report: In-depth Analysis*. Luxembourg: Publications Office of the European Union, p.96.

GAYLORD, M. and GALLIHER, J. (1987). *Edwin Sutherland and the origins of differential association theory*. New Brunswick, N.J.: Transaction, pp.1-184.

GOODMAN, M. (2015). *Future crimes*. 1st ed. London: Bantam Press, pp.1-682.

HAECK, P. (2017). Drugsbende spant top-IT'ers voor kar. *De Tijd*. [online] Available at: https://www.tijd.be/tech-media/algemeen/Drugsbende-spant-top-IT-ers-voor-kar/9959382 [Accessed 28 Mar. 2018].

Home Office (2013). *Cyber Crime: A review of the evidence*. London: Home Office, p.5.

HUYBRECHTS, P. (2018). Antwerpen overspoeld door wit poeder. *Het Nieuwsblad*.

KERKHOFS, J. and VAN LINTHOUT, P. (2015). *Cybercrime*. 1st ed. Brussel: Uitgeverij Politeia nv, p.97.

LEFELON, P. (2017). Vlaamse top-IT'ers in klauwen drugsmaffia. *Het Laatste Nieuws*. [online] Available at: https://www.hln.be/de-krant/hoe-raakten-drie-vlaamse-top-it-ers-in-de-klauwen-van-turkse-bende-die-zeker-twee-ton-coke-en-een-ton-heroine-het-land-binnensmokkelde~a33c0f42/ [Accessed 28 Mar. 2018].

LEUKFELDT, E. (2017). *Research agenda The human factor in cybercrime and cybersecurity*. The Hague: Eleven International Publishing, pp.1-95.

PASTERNACK, A. (2013). To Move Drugs, Traffickers Are Hacking Shipping Containers. *Motherboard*. [online] Available at: https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs [Accessed 26 Mar. 2018].

ROBERTSON, J. and RILEY, M. (2015). The Mob's IT Department. How two technology consultants helped drug traffickers hack the Port of Antwerp. *Bloomberg*. [online] Available at: https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/ [Accessed 25 Mar. 2018].

SYKES, G. and MATZA, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6), p.664.