# The Internet of Things is in rapid development; are we aware of the risks that follow?

**An empirical thesis**

**BACHELOR THESIS (BOPPG30)**

**The Norwegian Police University College**

**2020**

Student nr.: 971

Words: 6583

# Table of content


1. Introduction ..... 4

1.1 Choice of topic ..... 4

1.2 Scope of the thesis ..... 5

1.3 Clarification of concepts ..... 5

1.3.1 Cybercrime ..... 5

1.3.2 Digital forensics ..... 5

1.3.3 Digital murders ..... 6

1.3.4 What is a Hacker? ..... 6

1.3.5 The Internet of Things ..... 6

1.4 Outline and structure of the thesis ..... 7

2. Theory ..... 7

2.1 The security level on a pacemaker's ecosystem ..... 8

3. Method ..... 9

3.1 Choice of method ..... 9

3.2 Knowledge in advance ..... 9

3.3 Choice of units and variables ..... 10

3.4 The structure of the questionnaire and pre-test ..... 10

3.5 Implementation of the questionnaire and response rate ..... 11

3.6 Validation and reliability ..... 12

3.6.1 Sources of error regarding making the questionnaire ..... 12

3.6.2 Sources of error regarding distributing the questionnaire ..... 13

4. Presentations of the results and discussions ..... 13

4.1 Do the Norwegian police students know what happens with a patient's pacemaker when they are involved in deaths of people with pacemakers? ..... 14

4.1.1 Attention given by province ..... 15

4.2 What advantages and disadvantages do the Norwegian police students see regarding the rapid development of the IoT? ..... 17

4.2.1 Competence and knowledge about the IoT ..... 17

4.2.2 Awareness of the possibility of remote control and digital murders ..... 18

4.3 Do the police students find it possible to kill a person by hacking their pacemaker? ..... 18

4.4 Started the survey but did not finish ..... 20

5. Conclusion ..... 20

Bibliography ..... 22

Chosen curriculum ..... 22

List of figures ..... 23

Appendix 1: Questionnaire ..... 25
Appendix 2: Translation to the text answers rendered in section 4. ..... 27

# 1. Introduction

*"The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life."*

Bill Gates (Green, 2014, page 30)

We live in a digital age and every day the internet opens a world for us which we can do with what we please. And often, we do not think about that internet is such a big part of our lives, because we don't even notice it. The majority of the population is using these online connections to perform harmless actions, like using social media, play games or read up on today's news. But as easy as ordering takeout online, is ordering drugs and having them sent to an address of your choice. Even ordering a hitman to murder your neighbour is quite accessible.

These unlimited possibilities piqued my interest, as well as the following question: Where does it stop? I started looking into the possibility for something not mentioned by many yet, digital murders. Specifically, murders committed by a hacker using digital platforms to gain unauthorized access to medical devices, with the main focus being the misuse of pacemakers.

## 1.1 Choice of topic

Since the age of 14, I have been a gamer and have lived a life online that is equally important to me as my real life. This has given me an insight in several online communities and how easy it is to hide who you are and what you do online. As a preparation to write this thesis, I applied for a student scholarship to the Black Hat conference in London in December 2019 (Black Hat, 2020) and they awarded me with one. This conference gave me even more motivation to write a paper on digital murders.

I picked this subject because in my experience it is largely overlooked by the average police officer. While working as a police officer during my second year of police education we experienced several deaths involving people who wore pacemakers. We did not open cases for any of these deaths since they were considered to be of natural causes.

There is not a lot of talk about the possibility of digital murders. The example with the pacemakers is one of the worst-case scenarios, but as a police officer the worst case is what one need to prepare for.

## 1.2 Scope of the thesis

This thesis is about the police student's awareness about serious crimes committed online. The scope of the thesis is:

> *"The Internet of Things, IoT, is in rapid development; are the Norwegian police students aware of the possibility that it might be used as a murder weapon?"*

I have composed three research questions to help me illuminate this scope.

1. Do the Norwegian police students know what happens with a patient's pacemaker when they are called out on assignments involving dead people with pacemakers?
2. What benefits and disadvantages do the Norwegian police students see regarding the rapid development of the IoT?
3. Do the Norwegian police students think it is possible to kill a person by hacking their pacemaker?

As the research questions show, I have picked one possible way of using the Internet of Things as a murder weapon: Hacking a pacemaker and it's eco environment, which I will explain under section 2.3. I have chosen to do a study on today's police students, because they are the police of the future. If there is awareness amongst the students, they will drag that awareness into the workplace.

## 1.3 Clarification of concepts

This is a paper about digital police work. There are a few terms I'm going to use throughout this paper that I would like to clarify.

### 1.3.1 Cybercrime

To define cybercrime is not an easy task. Thomas Holt and Adam Bossler (2014, page 21) wrote in their article that there is *"no single, agreed-on definition of cybercrime, many scholars argue that it involves the use of cyberspace or computer technology to facilitate acts of crime and deviance."* I find this to be a good way to describe cybercrime. In short, it's a crime that are being committed by using or being on the internet.

### 1.3.2 Digital forensics

Digital policework seeks to safeguard the use of digital information and digital evidence. Digital evidence is per definition: *any digital data that contains reliable information that can support or refute a hypothesis of an incident or crime* (Årnes, 2018, s.7). This is data gathered from digital devices that we carry around with us, have in our houses or are available at public

places. In society today there are digital devices everywhere, and the amount of possible digital evidence is enormous. While working as an investigator in my second year of education, I experienced that the police were using a lot of digital evidence in trials, e.g., phone records, picture information and surveillance tapes.

The digital forensics process is a five-step chain which consists of identification, collection, examination, analysis and presentation of the results (Flaglien, 2018, page 16). This paper will focus on step 1: Identification. The awareness among police students that makes the identification of a digital murder possible.

### 1.3.3 Digital murders

Digital homicides in this thesis are homicides committed through the Internet of Things. Acting from a distance, using the devices' software and the connections between devices to disrupt and/or change the information on the device with a fatal result. These types of murders are committed by a black-hat hacker, see section 1.3.4, either with help from an acquaintance of the victim to gain access to the password of the device, or by brute forcing the device's security. I will elaborate further on this in section 2.1.

### 1.3.4 What is a Hacker?

A hacker is no longer only a hacker. From the traditional geek that knew all about computers, the term hacker has evolved into something different. There are few hackers left, and those are often linked to something criminal. These are the ones that we refer to as black-hat hackers, hackers that have malicious intents when trying to gain access into different systems. On the opposite side we have the white hat-hackers, often referred to as ethical hackers. These hackers work for companies and organizations and have permission to attack their systems with the goal of finding security risks before the black-hat's find them (Nanda, 2019, page 285-286). To know what a hacker is, is necessary to understand who is committing these digital murders, and how they can be committed. In this thesis, when the term "hacker" is used, it referes to the black-hat hackers.

### 1.3.5 The Internet of Things

The Internet of Things, from now on referred to as IoT, is a term that is used for the network of things, or devices, that is connected to the internet and each other though different network protocols (Sandvik, J, 2018, page 192). This can be your phone and tablet, but also your fridge, TV, toothbrush or pacemaker. The IoT is the reason that you can sit on your couch and

control the lights in your entire house. Or check if you remembered to lock your front door from your desk at work. Of course, this is helpful in your day to day life, but how safe is it?

Having medical devices, like insulin pumps and pacemakers, connected through the IoT can make it easier for the patient, but it brings with it some concerns. The security level on these medical devices can vary, and are dependent on a few different things, like what kind of device and manufacturer. For the rest of this paper I will use pacemakers as an example. When using the word pacemaker in this thesis, I am referring to implantable devices that helps to regulates a patient's heartbeat, including implantable cardioverter defibrillators. I choose to use the one term to cover these different devices to slightly simplify a very complicated topic for the sake of this paper.

### 1.4 Outline and structure of the thesis

The topic of online crime is enormous, and to try to grasp it all would not be possible. This paper will be using one of the most serious crimes, murders, as the base for my research. More specifically murders committed by hacking into devices connected to the internet in an attempt to end a person's life. I will not discuss any other type of online crime. Furthermore, the deaths following bullying or encouragement from online sources are not considered as digital murders in this thesis and is therefore not discussed.

There are many ways one can imagine criminals to successfully kill a person using the IoT, examples include hacking into a car's computer, into a patient's insulin pump or even their pacemaker. To cover them all would be too much work for one research project. Thus, I have chosen one focus area, the hacking of pacemakers. Before presenting my research, I will present the theoretical background on the possibility of digital murders necessary to understand why this research is relevant.

This is an empirical thesis where I have conducted a quantitative survey on my fellow police students to illustrate the awareness regarding the Internet of Things and how it can be used as a murder weapon. I will present my research in section 4: Presentation of results and discussion.

## 2. Theory

The society is facing a more complex world now than ever, which means police work grows more complex as well. This challenges the traditional ways of policework and demands more of each and every police officer in the streets (Hesthave, 2016, page 162). The digital

development is a big part of this complex world and has been in evolving continually for several decades.

## 2.1 The security level on a pacemaker's ecosystem

Several pacemakers today are connected to a Home Monitoring Unit, from now on referred to as an HMU. An HMU is a small computer that collects data from the pacemaker and send them to the pacemaker's manufacturers server. Specialized doctors can then review this data from a web surface to check that the heart if acting like it should (Kristiansen & Wilhelmsen, 2018, page 2). If the pacemaker is picking up irregularities in the patient's heartbeat or if the pacemaker is reporting a defected battery, the doctor can ask the patient to come in for a check-up.

But what happens if a third party decides to attack the pacemaker's HMU? One of the concerns is that by doing so, a hacker can possibly interfere with the pacemaker's frequency or stop it completely, with the consequences of it being fatal to the patient. In fact, MedSec, a cybersecurity firm, demonstrated in 2016 two cyberattacks on implantable devices manufactured by St. Jude Medical that could prove dangerous for the patient, including a "crash attack" that cause the device to malfunction and an attack to drain it's battery (Muddy Water Research, 2016, p.2-3).

Kristiansen & Wilhelmsen (2018, page 3) have done research on security system of the pacemaker's ecosystem, which includes the pacemaker, a pacemaker programmer (which is a computer used to program the pacemaker) and optionally an HMU. Their research concludes that "*the security level of the pacemaker ecosystem is inadequate".* They were able to find 194 critical vulnerabilities which makes it insecure (Kristiansen & Wilhelmsen 2018, page 93).

Their research is a part of a larger project on medical devices at SINTEF and initiated by Marie Moe (Snøfugl, 2017). During the process of writing my thesis, I got connected with a researcher named Guillaume Bour, who is supervising the ongoing work on pacemaker security at SINTEF. I got to read his master thesis "*Security analysis of the pacemaker home monitoring unit: a BlackBox approach",* which is under embargo. One of the research questions in his thesis was whether or not it is technically possible to make an attempt against a person's safety, and what it would take for an attacker to do so (G. Bour, 2019, p. 8). In his research he found several vulnerabilities that could impact the patient's safety and privacy (G. Bour, 2019, p. 131).

Another important contribution to this topic came from Barnaby Jack as early as 2013. He developed software that allowed him to remotely send a shock to anyone with a pacemaker within 50 yards. When questioned about the software, he said that it took him about six months and that it takes a specialized skill, but that it is possible (Alexander, 2013).

The research that has been done so far shows us that the hacking of medical devices is not something that is part of a fantasy or something farfetched. It is reasonable to imagine medical devices being compromised. And as a bonus for the one doing the attack, there is little to no risk of getting caught. The deaths of patients with pacemakers will most likely be discarded as deaths due to natural causes, without any further investigation.

# 3. Method

## 3.1 Choice of method

I have chosen to write an empirical thesis because it gives the best answer to the scope (Dalland, 2017, page 51). There has been little research done on the topic of digital murders up until now, and no research done when it comes to the awareness of this topic among the police.

By writing an empirical thesis, involving gathering new information, I have the possibility to get a deeper understanding of the topic. The data I have gathered through the questionnaire is my primary source of information (Dalland, 2017, page 162). To give the readers an understanding of the subject I have also used information regarding the possibility of hacking a pacemaker's ecosystem. Among these sources is a master study done on the subject of hacking a pacemakers eco environment, which has been an important motivation for me in this prosses, *"Security Analysis of the Pacemaker Home Monitoring Unit: A BlackBox Approach"* by Guillaume Nicolas Bour, 2019.

My key syllabus is written in English. Some of the terms have no adequate Norwegian translation or equivalents. The topic is an international one, with international issues, consequently I see the English as the appropriate language for this thesis.

## 3.2 Knowledge in advance

We all have a certain knowledge in advance that we take with us when we start going deeper into any material (Olsvik, 2013, page 111). My knowledge and interest for the topic may

colour the way I as a researcher make the survey and read the results. This is something I am aware of from the beginning and that I work to prevent. Olsvik, (2013, page 112) tells me that I should strive to find information that contradicts my own views, and to keep an open mind. I have discussed this topic with some of my classmates and my understanding was that the general police students did not think of murders committed with the IoT is a possibility. This has shaped me in this process, but I stayed determined to maintain an as objective view as possible throughout this project.

On the topic of implantable medical devices, my knowledge beforehand was limited. I have had to read up on the subject to implement it in this research and have used several master theses to understand how they work, so I could conduct the research for this thesis properly.

The fact that I chose a quantitative and not a qualitative survey helps me being objective, I can let the numbers speak. What I do control is which numbers I include in the thesis, and I have to be aware of not letting my own wishes for the findings to decide what I present in this paper.

## 3.3 Choice of units and variables

Units, or responders, are the ones we are conducting the studies on, and variables are the specific characteristics among the units, in other words what I actually research (Johannesen, Tufte & Christoffersen, 2010, page 239-249). The units here are the police students form all three years, B1, B2 and B3. The variables are their awareness regarding the possibility for digital murders committed through the IoT.

## 3.4 The structure of the questionnaire and pre-test

I started out wanting to do a quantitative study with a pre coded questionnaire because in my view, that approach answered my scope and research questions best. At the same time the results from this kind of test would be the most straight forward for me as the researcher to interpret (Johannessen, et al., 2010, page 261). I did a pre-test on three fellow students to test the questionnaire (Johannessen, et. al., 2010, page 274). These students did not answer the main survey when it was conducted.

During the prosses of making the questionnaire and performing the pre-test I experienced that I did not answer my second research question good enough by only using numbers. There are so many benefits and disadvantages to the development of the IoT that trying to limit this it to closed questions with set answers was not beneficial. This resulted in adding one question where I asked for a text answer from the participants and the final questionnaire was semi

structured, consisting of both open and pre coded questions (Johannessen, et al., 2010, page 261). I have experienced this as valuable, because some of the responders were very engaged in the topic and gave elaborate text answers that helped me in the research process.

The reason that I chose a questionnaire is that I can gather information from a lot of students in a short time (Johannessen et al., 2010, page 259). It has also been crucial to the research that I could do it from home, since the school and most of society was on lockdown for a long period during the time of writing due to Covid-19.

I have used www.onlineundersokelse.com as a tool to make the questionnaire. In addition to it being an easy and user-friendly platform for me as a researcher, it makes sure that I have no way of identifying any of the responders. Additionally, I have not asked for any directly identifiable data from the responders. As a result, this project is not covered by the Norwegian Personal Data Act. Therefore, I did not need to report it to the NSD, the Norwegian centre for data research (NSD, 2020).

## 3.5 Implementation of the questionnaire and response rate

I used the school e-mailing system and closed sites on Facebook to distribute the questionnaire on the 13th of March. I sent the survey by e-mail to a total of 1814 students by e-mail. In addition to that, I posted it on Facebook to our two closed groups for police students currently in B1 and B3. The e-mail and the post on Facebook consisted of a short explanation on what the survey was about and a link to the questionnaire. All units got a reminder on e-mail on the 19th of March with a deadline on the 25th of March.

Out of the 1814 units, 559 is in B1, 549 is in B2 and 706 is in B3. The class of 2017, B3, is bigger than the two following. This is something I am aware of when discussing whether or not the responders are a representative selection of the population (Johannesen et al., 2010, p. 241).

I got 474 responses, a response rate of 22,36%. Using the number of units in the mailing lists for each year, the response rate of B1, B2 and B3 is 32%, 19% and 25%, respectively. To find that the B2 response rate the lowest was not surprising. They did not get notified about the survey other than on e-mail, and I know from experience that B2 students don't check their mail regularly. Because of the slight variation in the response rate from the three years, the survey is not as representative for the entirety of the units that it could have been (Johannesen et al., 2010, p. 241).

In my opinion 22,36% is enough to give an idea about the awareness amongst the police students.

## 3.6 Validation and reliability

It's important to be aware that the data is not an exact replication of reality, only a representation of it (Johannesen et al., 2010, p. 36). The validation and the reliability of the data is important in every research project, to make sure the representation of reality is as accurate as possible.

The validation of the research means that we must be true to our scope (Thurén, 2009, p.32), to research the questions we want answered, and be aware of how relevant the research is. The validation tells us something about the quality of the research but must not be seen as absolute (Johannesen, 2010, p.71).

Reliability means the accuracy of the data gathered (Thurén, 2009, p.31). In other words, how I gathered the data, and what data I have chosen to discuss as results of the research. There are several ways of testing the reliability of the data, amongst those a test-retest. To perform the same research twice at two different times. Another is if several researchers are researching the same phenomenon. If they come to the same conclusion, the reliability is high (Johannesen et al., 2010, p.40).

I have tried to make sure my research holds a high standard of validation and reliability. However, I acknowledge that there are several things during this process that can compromise the validation and reliability of this research. I am going to explain some of these possible sources of error below.

### 3.6.1 Sources of error regarding making the questionnaire

One obvious source of error regarding the making of the questionnaire is my own inexperience as a researcher, as this is the first quantitative research I am conducting. To compensate for this, I have been in contact with the research department at my college and asked my supervisor on this thesis for guidance. They gave input on which questions to ask and how to phrase them.

Another source of error is related to the topic itself. Digital crimes and the IoT can mean different things to different people. From experience I know that some people run in the other direction if the topic of digital police work is mentioned, so there is a possibility that those who takes the time to answer the questionnaire are interested in the subject already and

therefor have more knowledge than the general police student. In an attempt to get answers from more than the interested students, I wrote in the email that there were no requirements regarding previous knowledge, and that all responses were valuable.

I also had to understand how implantable medical devices such as pacemakers work, and how they can be hacked. This was challenging as well. An error can occur if I have understood the facts wrong.

I found making the questionnaire challenging, because I wanted to research the awareness amongst the police students, and at the same time they would have to be given some information about the topic in advance to understand what I wanted to have answered.

### 3.6.2 Sources of error regarding distributing the questionnaire

I sent the questionnaire to several e-mail groups, not to single individuals. As a result, I can't know for sure who received the e-mail. The questionnaire was sent to 1814 units, and the Police University College reported 1885 students the fall of 2019 (Norwegian Police University College, 2020). This shows that I may not have reached all students. Therefore I also used Facebook and posted the questionnaire in two groups for students in B1 and B3, with 1102 members in total, in an attempt to limit this source of error. I also specified that the survey was for police students, just in case someone not enrolled in the university college got the link.

The fact that the students currently in B2 did not get any other notification about the survey than on e-mail is another source of error. This reflects in the results as well, 19% of the B2 students have answered the survey, while the numbers for B1 and B3 is respectively 32% and 25%. To present the result, I'll be using the number of students on the e-mail list as base numbers for the units.

Another source of error is that question three to six are only for B2 and B3 students. That means that they get more information about the topic before starting on question seven, which is for all responders. This can colour their responses because their thoughts may already have been directed in a specific way.

## 4. Presentations of the results and discussions

In the main part of this thesis, I will answer the research questions I presented in point 1.2 in the order they were presented. I will include relevant theory and previous research in my discussion. Furthermore, I will take a look at the variables I have in my research, which year

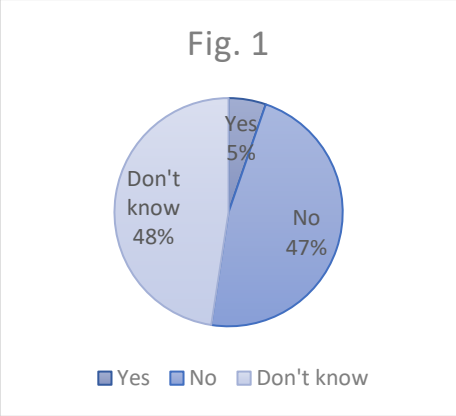
the participants are in, and which district they worked in during their second year and see if that has any impact on the awareness on this topic.

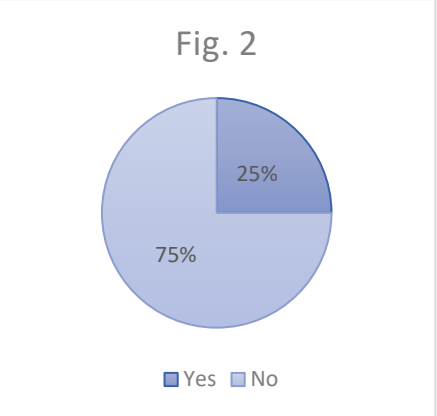
I asked questions in the questionnaire specified towards hacking of pacemakers but also regarding the IoT in general. This is because I think that a general awareness about the IoT is important as a base knowledge to be able to have an awareness about digital murders. It's all connected, and it's hard to research digital murders without the connection to the IoT.

## 4.1 Do the Norwegian police students know what happens with a patient's pacemaker when they are involved in deaths of people with pacemakers?

When I sent out the questionnaire, I thought that this question would have the lowest amount of responses, simply because it required the participants to 1; have had missions involving dead people, and 2; know if the deceased had a pacemaker or not.

78,8% (227 responders) have had missions involving dead people. Out of those 227 that answered affirmative on both questions, 5,3% (12 responders) answered yes to *"Did one or more of the dead had a pacemaker?"*, and 47,1% (107 responders) answered no.




Out of these 12 that answered yes, 3 participants answered that they knew what happened with the pacemaker. Their answers were: "Operert ut på stedet av lege", "Den ble tatt ut av lege" and "kuttet snitt, tatt ut. Den skal visst alltid ut før personen kjøres videre». This answers what is happening with the pacemaker on the site, but none of the participants said

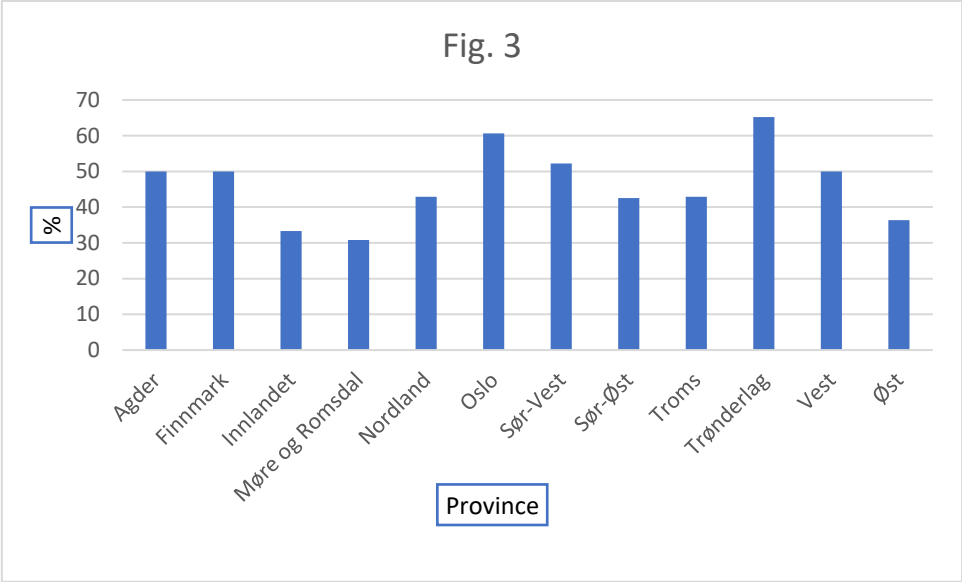
anything about what is happening with the pacemaker after that. Where it was sent to and what was done with the device itself.

As a police officer, we have access to the police intranet and KO:DE, which is a knowledge pool on what to do in different situation. There are a lot of valuable information to be found about what to do when you are facing a death in general. The police in Norway have good protocols when it comes to murders, and those investigations are taken very seriously, as they should be. I am therefore surprised by the fact that I haven't been able to find any information about the possibly of digital traces in medical devices, cars and other items that could be a tool to kill somebody, and what to do with them as a first responder.

52,4% was aware if the patient had a pacemaker or not. The remaining 47,6% (108 responders) did not consider checking it. That 47,6% answered "I don't know" might not be surprising regarding how little information there is to be found about the possibility of digital murders. Nearly half of the students do not think about checking if the dead have a pacemaker or not when they are out on a mission. As argued for in section 2.3, the hacking of pacemakers is not a farfetched thought, but it is reasonably new. And so far, it demands that the police officers have a previous interest in the digital crimes to grasp the possibilities and dangers about the IoT, because there is so little information given by the police as an organization.

### 4.1.1 Attention given by province

Figure 3 below shows how the 47,6% who did not consider checking for a pacemaker divided amongst the provinces. The percent that answered "I don't know" varies between 30,7% and 65,2% respectively in Møre og Romsdal and Trønderlag.




As shown, there is a slight difference between the provinces. When working in B2, you are connected to one supervisor the entire year, and the interests of your supervisor often is what you learn the most from. And the habits and routines at the station also affects it. All stations, and therefor counties, have their own priorities, which can influence the awareness about specific types of crimes.

The first phase in the digital forensics process is the identification phase, which includes detecting and recognizing a crime (Flaglien, 2018, p. 17-18). It is self-explanatory that if a crime is not detected, it does not get investigated, so one might claim that this first step is the most important. We could be missing detection of one of the most serious crimes we have, because we do not think that it is a possibility in todays society.

Amongst the documents found on KO:DE, is a checklist of what to do when you are facing an unexpected death, which I myself used during my second year. This gives the police on scene a run through of what they should be checking, including superficial medical records, and possibly clues you can find at the scene. This does not include checking for implantable medical devices or to make a note whether the car they sat in had an operating system that is a part of the IoT or not. The fact that there is little to no information about these things on KO:DE can contribute in explaining why there are so many responders that do not check if the deceased had a pacemaker or not.

## 4.2 What advantages and disadvantages do the Norwegian police students see regarding the rapid development of the IoT?

To answer this, I asked an open question where the responders didn't get any limits to what they could write. Out of the 474 that started the survey, 59% (280 responders) answered this question. I had 280 text answers to analyse, which makes the analysis more complex than if I had given them closed questions like the questions above. That being said, there are responses that are reoccurring and that are worth discussing.

When answering this, the responders from classes B2 and B3 had already answered some questions about death and pacemakers. This was done intentionally to get answers on questions three to six before giving a short explanation on the IoT. This may, however, have influenced how they answered question seven. I take that into consideration when presenting this part of the results. I will therefor separate my findings on B1 from B2 and B3.

### 4.2.1 Competence and knowledge about the IoT

One reoccurring answer is comments on the competence and knowledge about the IoT amongst the police force in general. Some of the answers were: «Dette har politiet svært lite kunnskap om/ligger langt etter i beredskapsplaner, tiltak, mv.», «… utviklingen går fortere enn politiet klarer å henge med på», «Manglende fokus og kompetanse» and «Kunnskap så langt baserer seg nok mer på interesse hos enkelte tjenestepersoner fremfor allmennkunnskap hos alle i etaten».

The comments about competence and/or knowledge in the police force in general about the IoT is made by students from all three years, but t's overrepresented by students from B2 and B3. These students have either had a full year or three quarters of a year working as a police officer. Therefor one can assume that the comments are a result of their own experience with the other police officers at their station. By working at a police station, you will get a sense of what that station and those police officers considers as important, and what the local challenges are.

As mentioned earlier, we are closely connected to our supervisor during the second year. There are no limits to what you may seek answers to yourself of course, but we are often tied up in the work we are set to do. If the supervisor does not have an interest for the digital murders, that might limit students developing that interest as well.

Which brings me to the comments about student's own competence about the IoT. Two students in B3 answered "Har ikke tilstrekkelig kunnskap til å kunne gi et svar på dette» and

«Jeg har problemer med å forstå hva internet of things er». These are students that have been attending the classes in digital police work both in the first and third year in school. Another B3 student writes that: «I tillegg er utdanningen man får på PHS ift DIGPOL et så dårlig undervisningsopplegg med lite oppdaterte lærere.». A student in B2 writes: «Jeg er ikke kjent med IoT».

To be prepared, we depend on learning about how to manage the digital crimes, what to look for and what objects that are important for the investigation. My initial thoughts were that students in B1 would have the least amount of knowledge about this to begin with, since they have the least amount of experience both regarding school and police work. The answers, however, suggest that that is not the case. In fact, not one of the comments about not having enough knowledge is from students in B1, only B2 and B3.

### 4.2.2 Awareness of the possibility of remote control and digital murders

Going through the answers, a few responders wrote comments directly pointed at the possibility for digital murders. Out of 280 answers, 8 responders, 2,8% mentioned the specific possibility for digital murders, either by hacking cars or medical devices. Among the comments were "Digital kriminalitet som er vanskelig å avverge/etterforske. F.eks. om en selvkjørende bil hackes slik at den krasjer.» and «Ting som er koblet til internett kan hackes …. For eksempel kan man tenke seg at selvkjørende biler kan hackes/fjernstyres til å krasje.». All of the 8 responders are students currently in B2 and B3. If this is because they have been asked about missions including pacemakers, or if that's something they would have answered anyhow is hard to say, but the fact that they mention cars and not pacemakers indicates that they could already be aware of the possibility of digital murder.

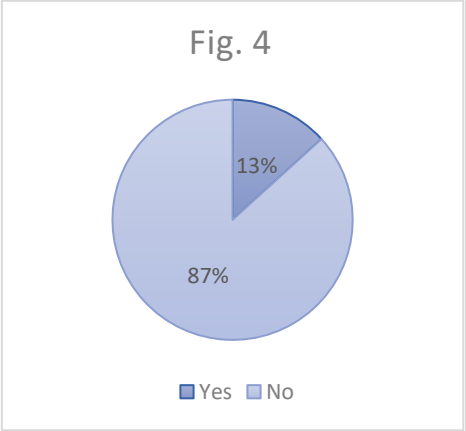
A few more students, 11%, mentioned hackings of different IoT devices and gaining remote control. These answers are divided between B1, B2 and B3 with 5, 14 and 15, respectively. The thought that hacking may be one of the disadvantages with the development of the IoT, I see as the beginning of believing there is a realistic possibility for digital murders. It takes skills within hacking to commit these kinds of murders, it is not an easy task as we can read from the interview with Barnaby Jack (Alexander, 2013).

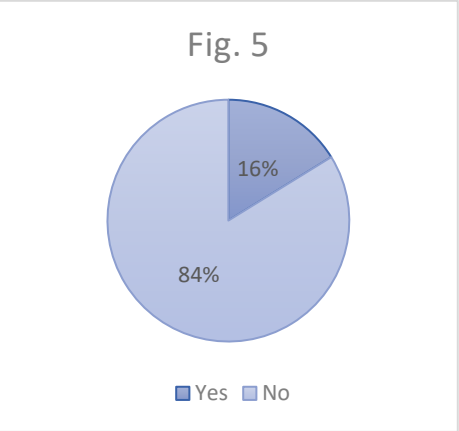
## 4.3 Do the police students find it possible to kill a person by hacking their pacemaker?

In the end of the questionnaire I asked two questions. Question eight: "Do you think it is possible for someone to gain unwarranted access to another's pacemaker by using the IoT?" and question nine: "Do you think it is possible to kill a human by hacking their pacemaker?".

There were 279 responders that answered question eight and 278 responders that answered question nine. I will link their answers on these two questions up to the text answers they gave in question seven.

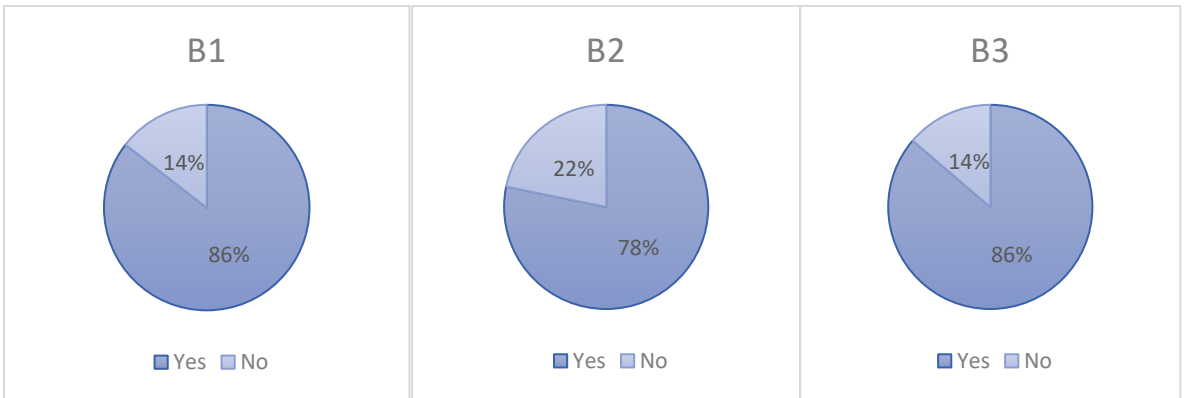
87% of the responders answered that they do think I's possible to hack someone's pacemaker, and 84% answered that they though it would be possible to kill somebody that way. This shows that given the direct question, a vast majority of the students can imagine the possible to commit digital murders.




These are interesting results when compared to the text answers the responders have given on question seven. While very few, 2,8%, uninvitedly mentioned the possibility of digital murders, 84% of the responders actually think that it is a possibility to kill someone by hacking their pacemaker using the IoT when asked directly about it. This shows that even though the awareness about the possibility of digital murders currently is not hight, the vast majority of the responders are open to the possibility of it.

Fig. 6:



There is a slight difference between the three years regarding the answers to question nine. The results from both B1 and B3 are that 86% think it's possible to kill someone by hacking their pacemaker. On question seven, none from B1 answered anything related to digital murders. When asked the direct question on the other hand, the amount that think it is possible is the same as the students in B3. From the students in B2, 78% answered yes, which is a bit lower than the other years. There is no obvious cause to explain this divergence.

### 4.4 Started the survey but did not finish

A surprisingly high number of responders started the survey but did not finish. Out of the 474 responders, 280 answered question seven. This is a drop-out rate of 59%. The 41% of those answering the first question dropped out of the survey before answering question seven. Before this question I gave a short explanation about the digital development and the IoT. The fact that so many people chose to not answer that question can imply that the topic is difficult, and they did not believe they had sufficient knowledge or competence to respond.

Though the answers given on question seven might give the impression that the students from B1 are more informed about the IoT than the students from B2 and B3, this might be misguiding. Out of the 182 B1 students that started the survey, 62%, 113 responders, did not answer question seven. This is a significant number of responders compared to B2 and B3 which both were at 27,7%.

I believe that in this case, the lack of responders that completed the survey is also an important finding, in and of itself.

## 5. Conclusion

In my research I have tried to answer the scope of this thesis: "*The Internet of Things is in rapid development; are the Norwegian police students aware of the possibility that it might be used as a murder weapon?"* By searching for answers to my three research questions I have looked for awareness amongst the police students regarding this subject. This is a difficult topic to researce because it is new and in rapid development. What is true today, might not be true tomorrow.

That being said, the research indicates that the general knowledge about the IoT and the possibility for digital murders by hacking medical devices such as pacemakers, is low amongst the students. The students see many advantages and disadvantages with the rapid development of the IoT and points out that knowledge is important to try to get a head of this

developing branch of crime, if possible, but few pointed out the option of digital murders. Being asked a direct question about whether or not they believe that digital murder by hacking a pacemaker is possible, a vast amount of the responders answered yes.

To imagine our smart devices being immune to hacking would be like burying our heads in the sand. If the device is online, one has to assume that it can be hacked. And we should prepare. After completing my research, I still think the awareness of digital murders is highly topical and further research on the topic would be valuable.

## Bibliography

Dalland, O. (2017) *Metode og oppgaveskriving.* Oslo: Gyldendal Norsk Forlag.

Flaglien, A. O. (2018). The digital Forensics Process. In A. Årnes (Red.), *Digital Forensics* (page 13-49). Hoboken NJ: John Wiley & Sons Inc.

Hesthave, N. K., (2016). Det forudsigende politi? In K.V. Rønn (Red.), *Efterretningsstudier* (page 161-195). Frederiksberg, DK: Samfundslitteratur.

Johannessen, A., Tufte, P.A. & Christoffersen, L. (2010) *Introduksjon til vitenskapelig metode* (4. edition). Oslo: Abstrakt forlag.

Olsvik, E.H. (2013) *Vitenskapsteori for politiet* (1. edition). Oslo: Gyldendal Akademiske.

Thurén, T. (2009). *Vitenskapsteori for nybegynnere*. Oslo: Gyldendal Norsk Forlag.

## Chosen curriculum

Alexander, W. (2013) *Barnaby Jack could hack your pacemaker and make your heart explode.* Retrieved from: https://www.vice.com/en_uk/article/avnx5j/i-worked-out-how-to-remotely-weaponise-a-pacemaker

Black Hat (2020). Black Hat Europe 2019. Retrieved from https://www.blackhat.com/eu-19/

Bour, G. N. (Under embargo). *Security Analysis of the Pacemaker Home Monitoring Unit: A BlackBox Approach.* (Mastergradsavhandling, NTNU). Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2623154. (151 pages)

Green, S. (2014) *Inside the mind of Bill Gates.* Dublin, IRL: Google Commerce Ltd. Retrieved from: https://play.google.com/store/books/details?id=wjiVBAAAQBAJ&rdid=book-wjiVBAAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport. (39 pages)

Holt, T. J. & Bossler, Adam M. An Assessment of the Current State of Cybercrime Scholarship. (20-40) Retrieved from https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_proquest1520331384&context=PC&vid=POLITIHS&lang=no_NO&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=

default_tab&query=any,contains,holt%20cybercrime&sortby=date&facet=frbrgroupid,include,8104535617407425760&offset=0. (20 pages)

Kristiansen, E.S. & Wilhelmsen, A.B. (2018). *Security testing of the pacemaker ecosystem.* (Mastergradsavhandling, NTNU). Retrieved from: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2609516. (143 pages)

Muddy Waters Research (2016). Report by August 25, 2016. Retrieved from: http://d.muddywatersresearch.com/content/uploads/2016/08/MW_STJ_08252016_2.pdf. (34 pages)

Nanda, s. (2019). World of White Hat Hackers. *International Journal of Scientific & Engineering Research Volume 10, May-2019*(5). 285-290. Retrieved from: https://www.ijser.org/onlineResearchPaperViewer.aspx?World-of-White-Hat-Hackers.pdf. (6 pages)

NSD (n.d.) Må jeg melde prosjektet mitt? Retrieved 18.03.20 from https://nsd.no/personvernombud/meld_prosjekt/index.html

Police University College (2020). Våre nøkkeltall for 2019. Retrieved from: https://www.politihogskolen.no/om-oss/fakta-tall/nokkeltall/?_t_id=7drEVvT5O35AUUqmuT7sHg%3d%3d&_t_uuid=EUz0t4BxTIC-05qKctXlVA&_t_q=antall&_t_tags=language%3ano%2csiteid%3a2df9291a-ada2-4678-a54b-5982a43383da%2candquerymatch&_t_hit.id=Content_Data_Pages_ArticlePage/_10ef2168-212f-4c19-98d2-a8a07efb8f79_no&_t_hit.pos=2

Sandvik, J. (2018). Mobile and embedded forensics. In A. Årnes (Red.), *Digital Forensics* (s.191-274) Hoboken, NJ: John Wiley & Sons Inc. (73 pages)

Snøfugl, I. (2017, February 15). Researchers heart problems uncover security gap. Retrieved from: https://www.sintef.no/en/latest-news/researchers-heart-problems-uncover-security-gap/

Årnes, A (2018). Introduction. In A. Årnes (Red.), *Digital Forensics* (s.1-11) Hoboken NJ: John Wiley & Sons Inc. (11 pages)

In total: 477 pages

## List of figures

Figure 1, *Answer to question 4*_____Page 15

Figure 2, *Answer to question 5*_____Page 15

Figure 3, *Difference between counties*_____Page 16

Figure 4, *Answer to question 8*_____Page 19

Figure 5, *Answer to question 9*_____Page 19

Figure 6, *Difference between years* _____Page 20

## Appendix 1: Questionnaire

**Question 1:** Which year are you currently in?

- B1
- B2
- B3

Question 2-6 for students in B2 and B3.

**Question 2:** Which district did you/do you work at in B2?

- Agder
- Finnmark
- Innlandet
- Møre og Romsdal
- Oslo
- Nordland
- Sør-Øst
- Øst
- Sør-Vest
- Troms
- Trøndelag
- Vest
- Annet, spesifiser:

**Question 3:** Have you had one or more calls involving deaths during B2?

- Yes
- No

**If yes, question 4:** Did one or more of the dead had a pacemaker?

- Yes
- No
- Don't know

**If yes, question 5:** Do you know what was done with the pacemaker?

- Yes
- Know

**Question 6:** If yes, what was done?

- Open text answer

Question 7-10 for students all years

Text given before question 7: The Internet of Things, IoT, is a term used for the network of all things that are connected to the internet. The digital development makes sure that increasingly more things can connect to the internet. This is done to make our day to day life easier.

**Question 7:** Do you see any benefits and/or disadvantages with the development of the IoT, from the police point of view?

- Open text answer

**Question 8:** Do you think it's possible that someone can gain unwarranted access to another's pacemaker by using the IoT?

- Yes
- No

**Question 9:** Do you think it's possible to kill a human by hacking their pacemaker?

- Yes
- No

**Question 10:** Any comments to the survey?

- Open text answer

## Appendix 2: Translation to the text answers rendered in section 4.

### Section 4.2.1

**Quote:** "Dette har politiet svært lite kunnskap om/ligger langt etter I beredskapsplaner, tiltak, mv.» **Translation:** The police has very little knowledge about this/are far behind in contingency plans, measures et.al.

**Quote:** «Utviklingen går fortene enn politiet klarer å henge med på».
**Translation:** The development is to rapid for the police to follow.

**Quote:** «Manglende fokus og kompetanse».
**Translation:** A lack of focus and competence.

**Quote:** «Kunnskap så langt baserer seg nok mer på interesse hos enkelte tjenestepersoner fremfor allmennkunnskap hos alle i etaten».
**Translation:** So far, the knowledge is based on interest from individuals, not common knowledge amongst everyone in the police force.

**Quote:** «Har ikke tilstrekkelig kunnskap til å kunne gi et svar på dette».
**Translation:** Do not have sufficient knowledge to answer this.

**Quote:** «Jeg har problemer med å forstå hva internet of things er».
**Translation:** I am having problems understanding what internet of things are.

**Quote:** «I tillegg er utdanningen man får på PHS ift DIGPOL et så dårlig undervisningsopplegg med lite oppdaterte lærere».
**Translation:** In addition is the education you get at the police academy lacking regarding digital policework, with professors that are not up to date.

### Section 4.2.2

**Quote:** «Digital kriminalitet som er vanskelig å avverge/etterforske. F.eks om en selvkjørende bil hackes slik at den krasjer,».
**Translation:** Digital crime that is difficult to prevent/investigate. Example: Self driving car is hacked and crashed.

**Quote:** «Ting som er koblet til internett kan hackes-…- for eksempel kan man tenke seg at selvkjørende bilder kan hackes/fjernstyres til å krasje.»
**Translation:** Things that are connected to the internet can be hacked-…- One can imagine that self-driving cars can be hacked.