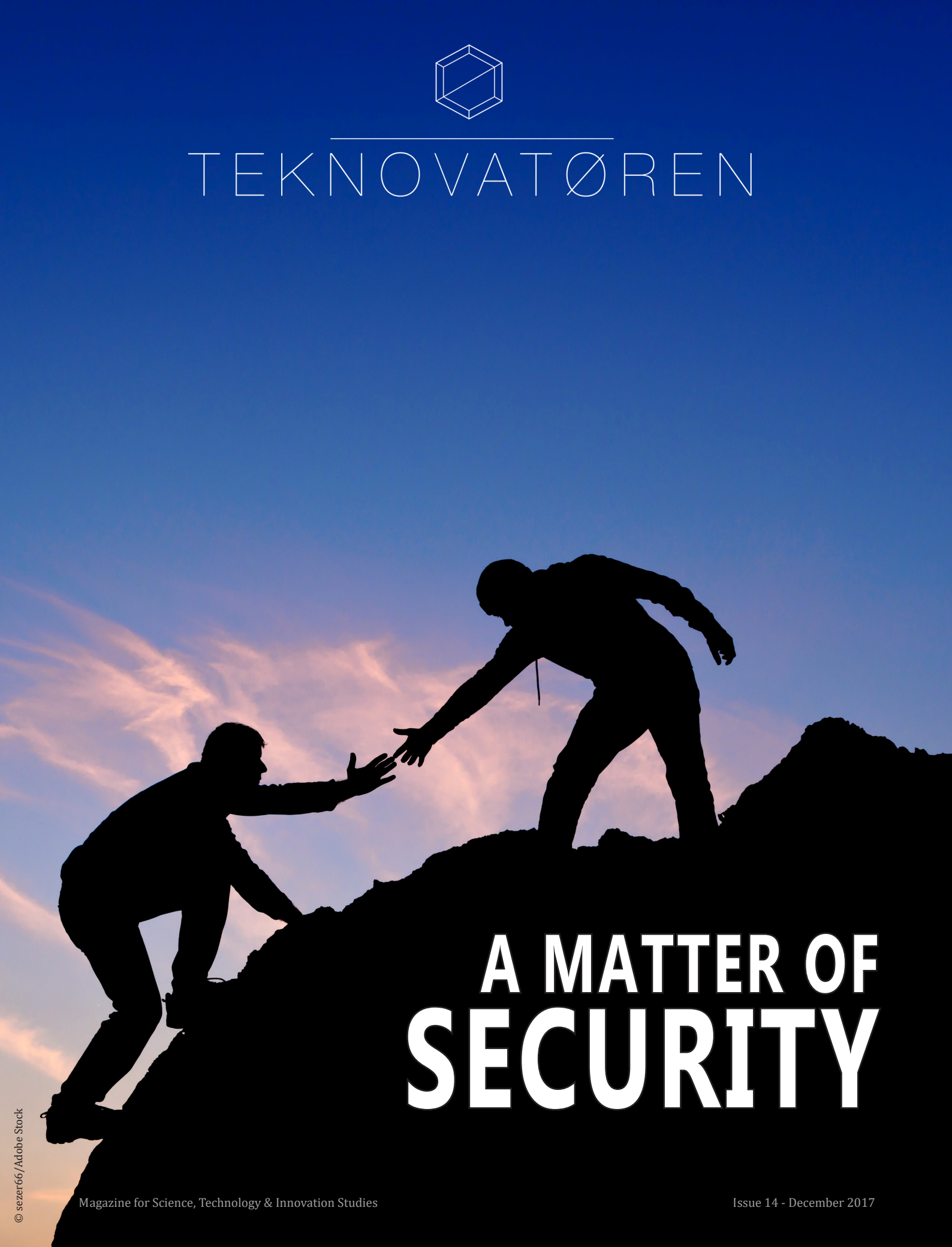
TEKNOVATØREN



A MATTER OF SECURITY

Magazine for Science, Technology & Innovation Studies

Issue 14 - December 2017

EDITORIAL

In this 14th issue of Teknovatøren, we shed light on some of the many issues of security in the digital age. We live in the most peaceful era of human history, and technological innovations - from the fire alarm to modern medicine - have contributed greatly to our safety over the past decades. However, this is not an indication that security in our time is a trivial matter. Quite the contrary. Ensuring continued safety brings new challenges as society becomes increasingly globalised and digitised.

In Maslow's hierarchy of needs, safety is the second-most basic human need, just above physiological needs. While Maslow is by no means a non-controversial figure, I don't find it unreasonable to argue that safety is more fundamental to humans than, for example, self-actualization. Keep this in mind as you read Ana Gviniashvili's article about the direction of the job market.

After working with different aspects of security during this past semester, it has become evident that safety and security is not just a matter of protection from immediate harm. Striving for security means dealing with threats such as constrained food supply, local pollution or cyber attacks, but our sense of safety also includes assurance that the authorities treat us fairly and look after our interests as citizens - also in the distant future. As technology and human lives become increasingly intertwined, it is important to pay attention to all of these issues. Learn more about quite effective, but potentially problematic technologies in Helge Neumann's article on biased big data, Nora Aagaard's article on privacy-infringing smart technology, or Jørgen Tresse's text on AI in pornopgraphy.

Furthermore, our experience of different threats to our security can be somewhat biased. Terrorism is one concern that shapes public debate and is among the security concerns that we take drastic and costly measures to address. Other issues, such as antibiotic resistance or global warming, have been relevant for a long time, but the security aspects don't seem as imminent to us and we struggle to deal with them properly. Hannah Monsrud Sandvik addresses humans' lack of ability to imagine the most extensive consequences of our actions in her article on the atomic bomb.

And finally, another reason why security is such a complex matter is that it always comes at a price. That price can be simply the annoying extra minutes needed to remember a password that is not just "Password". It can also, however, be the price of constrained privacy due to measures of surveillance to protect society from acts of crime. As society becomes more digitised, efficiencies come at the expense of increased vulnerability. The cost of ensuring future generations the chance to grow old on this planet involves restricting the use of our common resources. These deliberations are both everyday considerations and continuous debates about how we want our sociotechnical society to evolve. At the end of the day, it comes down to which safeties we value most, and whether or not we are willing to pay the price for them.

I hope you enjoy reading this issue of Teknovatøren. Be safe!

Siv Helen Egelund Gjerstad
Executive Editor

TEKNOVATØREN
#14

Authors:
Nora Vilde Aagaard
Marianne Areng
Susanne Bauer
Martin Beyer
Eirin Evjen
Siv Helen Egelund Gjerstad
Ana Gviniashvili
Sondre Jahr Nygaard
Helge Helguson Neumann
Christoffer Olsen
Hannah Monsrud Sandvik
Emilie Skogvang
Silje Totland
Jørgen Tresse
Anne Waldemarsen

A special thanks to Joar Kvamsås, Katie Coughlin and Emilie Pedersen Midtbust for critical input.

Layout:
Jørgen Aune

Illustrations:
Shutterstock
Adobe Stock
Alphabet King

Main sponsor:
Grønt Punkt

Additional sponsors:
Frifond
Studentparlamentet
Kulturstyret
Centre for Technology, Innovation and Culture (TIK)

Print: Allkopi, 700 copies
Published December 13th 2017

Teknovatøren is a semi-scientific magazine published by the master students at TIK Centre for Technology, Innovation and Culture, University of Oslo. Teknovatøren seeks to illuminate issues on technological development, innovation and knowledge production.

Find out more about us:
www.teknovatoren.no
www.facebook.com/teknovatoren/

Photo: Hannah Monsrud Sandvik

(Back row from left) Sofie Nebdal, Nora Vilde Aagaard and Tonje Kristiansen Sandnes.
(Front row from left) Jørgen Aune, Siv Helen Egelund Gjerstad, Marianne Areng and Even Dahl.

CONTENTS

EMPLOYMENT IN A ROBOTISED FUTURE

Ana Gviniashvili
TIK MA Student

Society today does not suffer from unemployment caused by too effective weaving machines.

The battle between humans and technologies counts centuries. Technological progress no longer means just machines doing repetitive work and drudgery, but AI technologies that are able to think and mimic cognitive behaviour. One day in the not too distant future, there might be a robot writing this kind of article, or driving our cars – to some degree, both of these examples are already happening. AI is already able to enter the job market in areas considered less likely to be automated in the past. As technologies are getting smarter and more humanlike at the same time as focus on automation amongst public and private sector increases, there is a rising concern regarding the future job market. Firstly, is automation a positive or negative thing for humans in the workforce, and secondly, will technologies actually replace human labour altogether?

Technological progress has always had a direct impact on employment and was a driving force in shifting jobs from agriculture to manufacturing, and onwards to service and management occupations. Despite the unemployment the technological development has caused while these transitions were happening amidst protests and anxiety, technologies had a positive rather than negative effect on long term wealth and social well-being. According to McKinsey & Company's report published in January 2017, it is estimated that between 1850-1910, productivity grew with 0.3% annually after implementing the steam engine. The same thing happened when early robotic and IT technologies were introduced and the resulting productivity growth reached 0.4% and 0.6% respectively.

The report predicts that the same thing will happen after the adoption of AI and robotics; by 2065 we're predicted to have an annual economic growth between 0.8% and 1.4%. In addition, while productivity grows, working hours are reduced by nearly 57%.

However, implementation of new technologies in companies is linked to unemployment. Due to the growth of artificial intelligence, both skilled and unskilled occupations are at risk of automation. Machine learning gives AI technology the ability to learn from experience without every step of the process being explicitly programmed. Thus, with enormous amounts of data, AI can enrich its experience way faster than humans, and can potentially carry out work that requires decision making, analysis or even creativity (eventually). According to McKinsey, in Norway, near 42% of working hours can be automated with today's technologies.

The potential of automation differs across activities and sectors. Frey and Osborne (2013) concluded that near 33% of jobs in Norway will be automated in a decade or two. Predictable, repetitive tasks, jobs with lower wages, and education are at higher risks. Examples include manufacturing, food service, transportation, accounting, bookkeeping professionals and general office clerks. Less likely to be automated are jobs with higher education, wage and specialisation – such as the people determining firm strategy, human resource functions, marketing, educational services, software developers, financial analysts, etc.

When considering what the job market will look like in a decade or two, it is important to note that automation of jobs does not necessarily mean that

© Sergey/Adobe Stock

whole occupations will disappear, but rather that some tasks within an occupation will be automated. For instance, fraud detection specialists in finance have changed their focus from looking through physical transaction records, and now work with training intelligent machines and designing increasingly fraud-safe processes. Their jobs still exist, but AI has freed up their time for other, value-creating activities. However, we have jobs that might disappear entirely, while new jobs arise in their place. For example, when self-driving cars are implemented there will be no need for drivers, but new jobs are created in design, development, monitoring, implementation of AI and robotics.

In general, it is difficult to measure exactly the difference between eliminated jobs and new occupations, but we have seen this kind of process before: Industrialisation, computerisation and now AI and robotisation. Every time we have invented technologies to take over human labour, people have shared the same fear of technologies taking over their niche in society. Regardless, what we have seen so far is that due to technological development, efficiency and productivity has grown, which has resulted in a better economy and higher standard of living. The people displaced with technological change eventually adjusted to the new reality after change had come about – the social unrest and short-term unemployment was largely affected by their ability to adapt and find a new role in society. Therefore, when we meet the disruption of robots and artificial intelligence, our focus should not be constraining development, but ensuring that the human part of the workforce has a high degree of flexibility and ability to adapt.

In this process, governmental and educational systems will play an important role and need to adjust in order to provide people with the opportunity to requalify themselves during their careers. Take the example of Singapore, which promotes lifelong learning and offers $345 credit to citizens over 25 that can be used to take a course at approved universities or online in order to remain competitive in a changeable, technologized job market.

In the end, the same question remains – will the robots take our jobs? I do not think so, but evidently, AI technologies and robotics challenge the traditional ways of employment, and being good at one thing no longer guarantees long-term employment. Nevertheless, history has taught us that smashing the weaving machines was not a good solution to unemployment, indicating that flexibility and openness to learning new skills will be key when facing the future labour market.

APOCALYPTIC BLINDNESS AND THE ATOMIC BOMB

Hannah Monsrud Sandvik
ESST MA Student

The mere existence of the atomic bomb carries with it the possibility of the complete annihilation of all forms of life. Through an investigation of the nature of the bomb, we can better understand the relation between technology and the effects machines have on our lives.

Technology is persistently praised for its ability to connect and unite us. In perhaps no case is this more apparent than with regards to the atomic bomb, which in an absolutely inclusive sense affects us all simply by existing. The increasing power struggle between the US and North Korea, and recent reports that the latter has successfully tested hydrogen bombs, only serves to underline the fact that the current atomic situation should be our greatest worry.

Few have written as extensively and profoundly about the atomic bomb as the Austrian philosopher Günther Anders (1902-1992). For Anders, the dropping of the atomic bomb on Hiroshima on August 6th, 1945, marked the beginning of an era where the entire world at any moment could be turned into post-nuclear ashes. The atomic bomb is more than a weapon of mass destruction: because the bomb makes it possible to obliterate all life on earth, we are confronted with a new existential condition. As Anders writes, "the possibility of our final destruction is, even if it never happens, the final destruction of our possibilities." (My translation.)

In the 1960s, Anders started a correspondence with Claude Eatherly, the American reconnaissance pilot who declared the weather conditions satisfactory to drop the bomb. Their writings were subsequently published in the book *Burning Conscience*, a collection of letters reflecting upon the human condition in the atomic age.[1] Eatherly was the living example of everything Anders thought about the bomb. After Hiroshima, Eatherly was celebrated as a war hero, but he struggled to come to terms with his role in the bombings. Subsequently he attempted suicide, went through a divorce and performed several armed robberies, though never actually stealing anything. In Anders' view, these were acts of repentance: a way of seeking a punishment Eatherly felt he deserved but didn't get.

The reason why the Eatherly case is so interesting is that it shows how technology turns us into cogs in large machineries and removes us from the relation between cause and effect. Anders calls the gap between our ability to imagine something and our ability to produce it the *promethean gap*.[2] The fact →

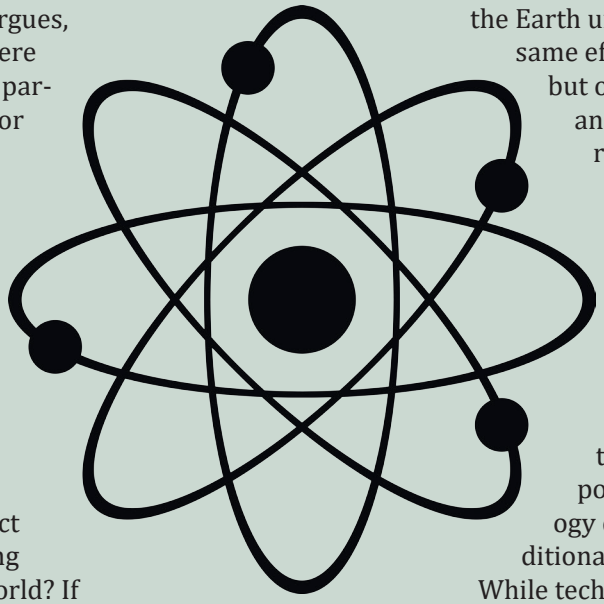
1 While this book offers insight into Eatherly's thoughts, it should be approached with a certain skepticism. Eatherly was in a psychiatric hospital during the time of their correspondence, and the two never met. More than two thirds of the book consists of letters written by Anders, and he can easily be accused of using Eatherly for his own agenda. All the same, the letters offers insight into Eatherly's thoughts and serves as a useful illustration of Anders' thoughts about the relation between the machine and its user.

2 Footnote introduction to Prometheus because of space restrictions: Prometheus was a Titan in Greek mythology who is best known for stealing fire from Mount Olympus and becoming the greatest benefactor of humankind, a pretty miserable group of people prior to this. The gift of fire, according to the usual interpretation of events, signifies technology and the beginning of humanity as we know it. The myth of Prometheus suggests that humans are unfinished beings who need artifacts in order to be in the world, and in his texts, Anders' uses this symbolism for what it's worth. (It didn't end well for Prometheus: Zeus became concerned with the growing power of mankind and decided to punish Prometheus for the role he had played in enabling this, so he chained him to a rock and had an eagle eat his liver, which regrew every night.)

Ruins of Nagasaki after the atomic bomb on the 9th of August 1945

Photo: © konstan/Adobe Stock

that I push the button seems unrelated to the fact that millions of people die as a direct result of this. It is paradoxical how pushing a button is easier than killing one single person, but this is the case because the larger the possible effect of a certain act, the more difficult it becomes to imagine the effect. Adolf Eichmann, one of the lead organizers of Holocaust, used this line of argument to make the case that he was not guilty for the role he played in murdering thousands of Jews - he was merely following his superiors' orders. In the Eatherly letters, Anders turns the argument around. Morally speaking, Anders argues, there is no such thing as 'mere co-acting' - whatever we're partaking in doing, promoting or provoking is being done by us, and using Eichmann's excuse is the same as abolishing the freedom of moral decision and the freedom of conscience. Eatherly's feeling of guilt, therefore, was an entirely appropriate response.



The underlying question is the following: How do we act when faced with the looming menace of the end of the world? If we know and understand the disastrous consequences of the bomb, why are we not doing more to stop it? The reason we are not currently collectively panicking, is that we are unable to imagine that the atomic bomb could strike and the consequences of this, even though it has already happened. In this sense, we are *inverted utopists*, to use Anders' terminology: while regular utopists are unable to produce what they imagine, we, on the other hand, are unable to imagine what we have produced. When confronted with things we cannot classify, we deal with them as if they didn't exist at all. The real menace, then, lies not in the bomb itself, but rather in our apocalyptic blindness towards it.

The only solution, according to Anders, is a radical expansion of our imagination - we have to bridge the promethean gap between the produced and the imagined.[3] This is not an exercise that is limited to space; we also have to widen our sense of time. While the bomb has contributed to making the world geographically smaller, it has also made the possible futures into neighbouring regions of our present time. Anders' argument can, for example, be extended to cover the effects technological advances and our consumption have on the environment. We are making the Earth uninhabitable, causing the same effects as an atomic bomb, but over a longer period of time and through a more complex relation of events, making the consequences even more difficult to grasp.

The critique of the bomb, then, is not limited to the atomic age. The atomic bomb, in Anders' view, is the archetype of all technology: It stresses the point that the more technology develops, the more conditional our existence becomes. While technological objects are often framed as neutral because they can be used for good or bad depending on the intentions of the user, they are in fact better understood as the configuring elements of the way we think, feel and interact with each other. Technology, as it turns out, is no longer a means to an end; it has become an end in and for itself and the real subject driving history. Each technological advance actualizes a possible world, but it remains to be seen whether there can be room for us in it.

3 Anders' own way of doing this is shown through his philosophical method, which is one of exaggeration. In Anders words: "If one were to amplify viruses a million times and screen their devastating workings, would this amplification of the format also co-exaggerate the danger? Or would the danger here rather become visible for the first time?."

FOREVER A PORNSTAR, SOFTWARE SAYS

Jørgen Tresse
TIK MA student

Judging by any benchmark, Julie is a normal teenager in school. During the course of one day, a series of unfortunate events left her social and private life in ruins. These events also led to her transferring schools and suffering from severe psychological trauma. What happened?

I made up the previous paragraph, but it is nonetheless based on true stories. Unfortunately, this is something that does happen.

It should come as no surprise that teenagers engage in sexual activities. However, in the twenty-first century, these intimate activities are not necessarily acts that stay exclusive only to the people involved. With the advent of social media and an increasing norm of sharing all the details of your life on the Internet, acts that may have been poorly thought through – or at the very least meant solely to be private – can be filmed or photographed and shared with hundreds of people within minutes. As *Aftenposten* has shed light on through a series of articles in the fall of 2017, it is not uncommon that youths share photographs and videos of sexual activities involving their peers. It even seems to be happening regularly, and involves a wide variety of young people. A common thread is that the persons exposed — often young girls pressured into an act — are unaware of this sharing. It is also striking how the common reactions boys and girls receive are as opposite as can possibly be: their peers praise the boy as a man, while labeling the girl a slut. The photo or video in question can be shared with the whole school within a day, and can even spread further, possibly ruining a person's social life through crowd judgement in the process. →


© Andrii Zastrozhnov/Adobe Stock

There are popular porn niches devoted to material where you know the identities of the persons engaging in sexual acts. The allure of recognising an actress is not lost on the Internet, with finding out the identity of people in pornographic videos or gifs being a hobby and skill several people pride themselves on. For example, you can find communities on the social and media aggregation website Reddit where users help each other to determine the name of an actress from a specific pornographic clip, or services like Pornstar.id where you can reverse image search porn stars. Recently, Pornhub – as of October 2017 ranked the 20th most visited Internet site in the US – announced that they are piloting an AI-based software that identifies specific porn actresses in clips. This is supposedly so that users can more easily find their favourite actresses and fetishes, and Pornhub claims that they will only use the software on professional actresses. However, as several privacy enthusiasts have pointed out, these new features should be worrying.

Teenagers sharing videos and pictures of each other is devastating for those involved, but unfortunately it is far from the only non-consensual sharing occurring. "Revenge porn" is a category of porn where jilted exes share intimate and private content without their previous partner's consent, and with the intent of shaming or hurting them in some way. This does not just affect an unlucky few – some surveys have revealed that as many as 23% of respondents, overwhelmingly women, have experienced being the victim of revenge porn, with pictures and videos being spread on an estimated 2,000 websites worldwide dedicated to this genre.[1] Often, this is accompanied by *doxxing*, or the release of private information such as full name, address, telephone number and more, opening the door for widespread abuse. While there are efforts underway to limit the damage from incidents like these — Twitter, for example, is banning profiles which engage in these activities, and the American Congress is considering making doxxing a federal offence — it is easy to see how software such as Pornhub's may exacerbate the problem.

It is common that a technology which is developed for a certain use, gets applied in other areas or by actors with other needs. Viagra, for example, was originally intended as a heart medicine, Listerine as a cure for gonorrhea, and the Frisbee was a pie container, but none of these uses are what they are best known for. Serendipitous discoveries happen a lot in the fields of science and technology, but one does not always stumble upon a new use; actors with malicious intent can actively search for ways to warp a technology to fit their needs.

If the facial recognition AI is used on private videos as discussed here, it can connect those videos to a person's full digital profile, making personal information all the more accessible. *Aftenposten* focused on youth culture where actions have led to the courtroom, but for Julie, the girl who had to transfer schools, this may be a small consolation. Starting over somewhere new or waiting until content is forgotten, is hard enough as it is, without making the content easier to find and tagging it to a person so that it can follow them through their whole life.

Common sense tells us that anything shared on the Internet is on the Internet forever. The least we can hope for is privacy through hiding in the massive overflow of content that is out there.

1 Cyberbullying.org; ABCnews.com

THE GOOD, THE BAD AND THE UGLY BIG DATA

Helge Helguson Neumann
ESST MA Student

There is a hurricane on its way. You run to the store to stock up on essentials, preparing for the worst. What do you buy? Strawberry Pop-Tarts, apparently.

Using big data, Walmart found out that Americans buy seven times as many Pop-Tarts whenever a storm is brewing. Also using big data, Google guides you away from traffic jams by collecting millions of cellphone signals. Facebook recommends top stories based on their vision of you; a vision consisting of codified numbers generated by the actions of you and your kind. The atoms of cyber-you. With these data, companies are able to make sense of a world that does not even make sense to us. But is it all for good use? Here's a good, a bad and an ugly example of how big data can be used.

Big data functions as follows: you take a huge amount of data, and then use a computer to run algorithms to find some sort of pattern in the mess. It is used to find trivial issues such as fast-food preferences at different times of the day (at night, women like Thai food, men like Turkish, and everybody loves pizza), but also for making morally tense choices, like categorizing people. The data itself is not dangerous, but our interpretation and usage of it can have dire consequences. When we choose to use big data for big decisions, we need to take into account that big data can be accurate and helpful, but also unfair and racist.

"Big data" has become a buzzword in recent years much due to its promising possibilities for firms and customers, government and citizens. It helps Walmart stock up on Pop-Tarts when a storm is brewing. It helps the Norwegian government reveal fraudulent behaviour in the welfare system. But maybe most promising is its use within the health sector. Using big data from search engines and deep learning artificial intelligence, Google are showing promising results in predicting cancer before doctors are able to. How do they do it? By looking at tons and tons of search data to find some patterns between search words and cancer patients. This is perhaps the biggest advantage of big data: the ability to find interesting and useful correlations where we previously didn't know there were any.

Not all big data can show these sorts of correlations. In some cases, the data is highly uncorrelated, but are still being used for decision-making. Back in 2012, Sarah Wysocki started her job as a teacher in Washington, D.C. After some time, she was evaluated and scored highly with her superior. She was motivating, good at teaching, and the kids liked her. Two weeks later she was fired. According to a recently implemented teacher evaluation system, IMPACT, she was not suited to be a teacher. As an addition to a human evaluation, IMPACT was put in place to look at data statistics, to better make decisions about which teachers to hire and fire. Unfortunately for Wysocki, the evaluation paid more attention to the data than the person. The data said in particular that she was not effective enough. However, when looking at the data, Wysocki had reason to be upset. A scatterplot of the "effectiveness" showed little sign of a consistent pattern, and looked more like a starry night in the desert. The data did not reveal a significant correlation, with an $r=0.25$, which is about the same as the correlation between height and ice-cream preferences.

Misusing big data can have great impact on individuals, costing them their jobs or excluding them from insurance policies. It is all based on the atoms of cyber-you, what you are, what you have done, and even more importantly, what people similar to you have done. When these characteristics include black, poor, and American, you are, according to big data, in trouble.

The American police have started to use predictive analysis based on big data sets. However, the statistics that are fed into the data sets are not always trustworthy. For example, while blacks and whites in America smoke marijuana at the same rate, black smokers are four times as likely to be arrested for it. Similarly, the police more frequently patrol poor, black neighbourhoods. More patrols lead to more arrests and more points in the datasets. And once in prison, chances are you will return.

Courtrooms in America are increasingly using big data to determine the likelihood of committing future crimes. ProPublica, a nonprofit investigative newsroom, dug into the numbers and found some disturbing news. The data were highly biased towards black people, automatically predicting black criminals to be more likely to commit future crimes. Not only were the predictions barely more accurate than a coin-toss, they were twice as likely to falsely accuse black people. Recently, American courtrooms have taken it a step further by using algorithms in the sentencing. Because of privacy protection, the defendant is not able to question the sentencing or view the algorithm or what data has been put into it.

Big data has an inherent risk of making history repeat itself. We use data from past experiences to predict the future, and in doing so we nudge the future in that direction. If Walmart finds out we bought Pop-Tarts during the last storm, they will put Pop-Tarts by the cashier before the next storm, making us more likely to buy them. If the police use datasets from poor, black neighbourhoods, chances are those same neighbourhoods will be targeted next. In the end, big data is only numbers. It is us that need to interpret the numbers, decide which ones to use and which ones to discard.

THE EDUCATION CRISIS – IS TECHNOLOGY THE SOLUTION?

Emilie Skogvang
TIK MA Student

There are currently 60 million children who do not have access to education, of which 30 million are living in areas affected by war and conflict. At the same time, there is a severe lack of teachers to meet the needs of these children. Can educational technologies, so-called "ed-tech", be part of the solution?

A question of safety and stability
When you think about the war in Syria, you might think of the millions of refugees who have had to flee their homes, the lack of food, the poverty and the primary needs that go uncovered. But did you ever think about the consequences of the 2.3 million Syrian children who have lost their opportunities for education due to the ongoing conflict? Even those children who do have access to school may face difficulties in learning because they have been under long-term stress, or because they may be taught in a language they do not master. How can Syria and other countries affected by conflicts ever hope to rebuild if millions of their people have had no access to education over long periods of time?

According to Save The Children, 60 million children are out of school globally. A further 60 million drop out before they reach 4th grade, and 130 million do not learn basic skills in the early years they attend school. At the same time, there are not nearly enough teachers to meet these needs, especially in fragile contexts characterised by war and conflict. According to the most positive forecasts, we will not be close to having enough teachers for the next 30 years. The trend is that many humanitarian crises turn into protracted crises, like the war in Syria. This means that the lack of education for these children is a long-term problem, and short-term solutions for long-term needs will simply not suffice. This is an under-communicated crisis which is not only a question of the psychosocial well-being, safety and the future of the millions of children affected by wars and conflicts, but also a question of global safety and stability in the years to come. These children will build the societies of the future, and we must make sure they have the right tools to do that in order to ensure safe and sustainable development, especially in unstable parts of the world.

Can the edtech industry be part of the solution?
Humanitarian organizations are increasingly looking to partner with the private sector to harness their innovation capabilities and technological expertise. In the context of education in humanitarian crises, there is one industry in particular that might have a solution to the education challenge: the "edtech"industry. This industry consists of companies who are suppliers of educational technologies which might meet some of the needs of the children affected by crises. One example is EduApp4Syria which started as an international open innovation contest facilitated by The Norwegian Agency for Development Cooperation (NORAD). The contest resulted in two open source smartphone applications with the aim of helping Syrian children with basic literacy in Arabic and improving their psychosocial well-being. Whether the apps will have a positive impact on these two factors is yet to be seen. NORAD is currently collecting quantitative data from the field to see the actual impact, but the qualitative feedback they have received so far is very promising.

Another example is the Norwegian edtech company, Alphabet King. They have developed a solution called "The Learning Lab". This is a collection of

200 unique educational apps and physical exercises in a reversed classroom where the children walk around at their own pace and do tasks on their own level. The apps are designed to be easy for children with different backgrounds to understand, and they can be used on tablets, smartphones and computers. Alphabet King is currently piloting "The Learning Lab" in Gambia, Uganda, Somalia and Kenya among other countries, and they have found that the solution gives good results for children regardless of their nationality and socioeconomic status.

Although there are tremendous possibilities in technology, both the edtech industry and humanitarian organizations know that an app alone cannot save the world. Children need contact with adults and a safe learning environment to prosper. It is important to emphasize that edtech cannot replace a teacher or a safe learning environment:

"Educational technology has great benefits when it comes to distributing learning and knowledge to people in parts of the world where access to education would normally be impossible, as most people have smartphones. Digital tools can never replace teachers and formal education, but in times of crisis and conflict, it can help provide learning regardless of time, space and level."

Hege Tollerud, CEO of Oslo EdTech Cluster

Getting to know the end user through strategic partnerships

When developing any type of technology, the end user is important. After all, it is the end user's problems one is trying to solve. In this case, the end users are children affected by wars and conflicts, and it is their situations and needs that must be taken into consideration. Culture and context-specific characteristics must be incorporated into the solutions at an early stage in order to achieve real impact and be sustainable. Since humanitarian organizations usually have great knowledge about children affected by war and conflicts, strategic partnerships between humanitarian organizations and edtech companies are important to develop long-term solutions to tackle the education crisis.

Image Courtesy: Alphabet King

DON'T SET 'PASSWORD' AS YOUR PASSWORD

Anne Waldemarsen
ESST MA Student

Ever since 2011, The Norwegian Center for Information Security (NorSIS) has made October the 'Security Month', as a measure to raise awareness and promote security-oriented practices in the aftermath of 'the Digitisation'. Are the technologies we use to work, communicate, and store information thoroughly secure? Is it easy for outsiders to access a company's computer systems? Are employees aware of what is at stake if hackers steal or alter sensitive information?

To discuss these questions, a large number of security conferences are arranged. If you've never attended one of these crisis-maximizing events - don't you worry, my friend. I've attended a fair share, and here follows a summary of a typical day:

08.30 - 09.00: Registration:
Show up at the right address but wait hesitantly outside for five minutes in case you see someone you know so you don't have to enter alone. Once inside, receive your name tag (which is misspelled) and pick up a free notepad and a pen that reminds you who sponsored this event (a private consulting company). The notepad makes you appear both sincerely concerned and curious, but you and everyone around you knows that you will pick up your phone and browse through emails long before the second speaker enters the stage, and that the real reason for your attendance is to at least look like you are planning on keeping up to date on security-measures, plus the free coffee and "snitter".

09.00 - 09.15: Host welcomes everyone/practical information:
Make sure you know where the fire escape is, yes, but more importantly: What route you can plan in advance to sneak out and fill up more coffee and put some grapes and biscuits into your pocket.

09.15 - 10.00: You are all in grave danger:
Some important CEO warning everyone in the audience about how unprepared you all are should a Russian hacker decide to attack you. He talks about how "technology has changed the way we live", and says something about the internet of things - which he describes as how everyone's refrigerator is connected to wifi and can be misused to open your front door. You nod as if this is a common concern to you. At the same time, you wonder how you have overlooked the fact that your refrigerator from 1991 apparently has wireless internet connection, and inherent bad intentions.

10.00 - 10.30: Comic relief:
Some unimportant IT-dude (which we later will learn is the real MVP) makes an effort to ease the tension, saying that your systems are sufficiently secure and that you and your company are not interesting enough to be attacked by a Russian or Chinese hacker. Even though this was meant to calm you down, you realise you feel somewhat offended and experience a need to prove yourself.

10-30 - 10.45: Coffee break:
Finally. You talk awkwardly with the man next to you, then run out to get some fresh air, hoping you don't look as tired as you feel. When back inside, you sit alone and feel unimportant since no one wants to hack your company. Then you count how many speakers are left before lunch break. You are excited about lunch, but slightly worried about small talk. Only one speaker stands between you and lunch: Some woman from The Norwegian

Business and Industry Security Council (NSR) talking about security measures.

10.45 - 11.30: A really long session:
The woman from NSR talks for forty-five minutes (!) about how you can behave in a safer way. This woman is abundantly more technically competent than you, with a Ph.D. from NTNU and a background in military intelligence. You are unable to keep up, so instead you desperately type "computer science" + "101" + "for dummies" + "continuous admissions" in the search engine on your phone. Lunch is right around the corner, thank God.

11.30 - 12.30: Lunch break:
You try to locate the nearest 7-Eleven because you remember how much you dislike snitter.

12.30 - 13.15: Everybody chill:
Some guy from The Norwegian National Security Authority (NSM) agrees with the IT-dude and says it is unnecessary to maximise the threat assessment. He explains how the media is making too much of a fuss about potential threats in cyberspace, and that private consulting companies will exploit your fear and offer you overpriced security packages.

13.15 - 13.45: Some good advice:
A woman from NorSIS, who seems tired of giving the same speech over and over again, informs the audience about how to act responsibly: "Always update to the latest version. Don't set "admin" as the password to the admin-user account. If your employees love the company, they are less likely to harm you when they don't work for you anymore." You look around at the other attendants and wonder whether someone really is stupid enough to need this information. Then you remember that the password to the workfile in your workplace containing sensitive health data is 'password'. →

13.45 - 14.00: Coffee break nr. 2:
Feeling sick of coffee due to overconsumption, you head for the tea-selection.

14.00 - 14.30: The sales pitch:
You remember why you never drink tea. A private consulting company representative brags about their experience in the field, lists all the catastrophes they single-handedly prevented, and states that 'WannaCry' was below their level of expertise. He continues to talk positively about how the state facilitates educating employees and making sure that Norwegian workplaces have the necessary tools to secure their digital systems, but that this might not be sufficient, and that if you really-really want to make sure that you don't lose sensitive information, which may lead to both your company and you as a private person being sued, you should hire this private company's security packages ASAP.

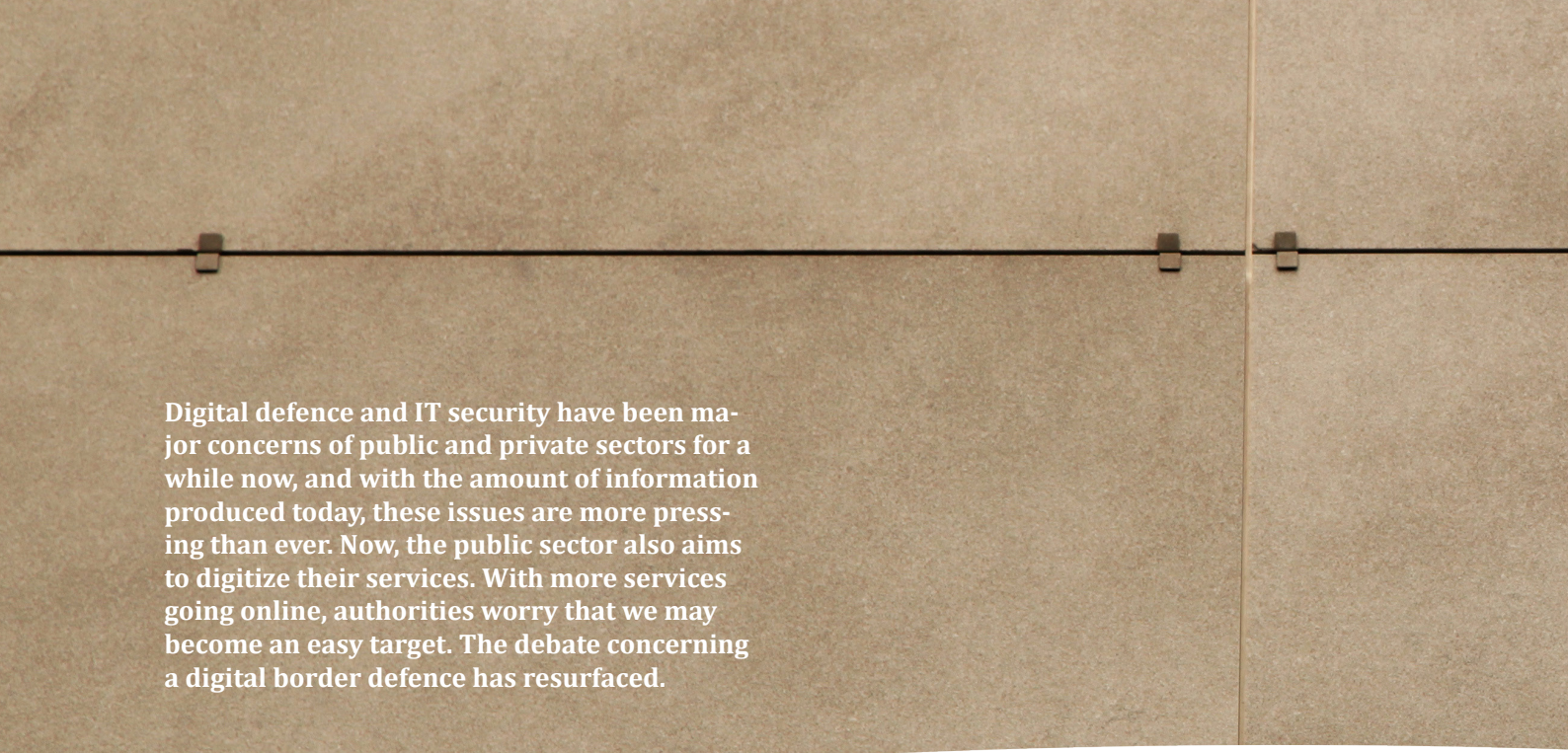
14.30: That is all:
Host thanks every speaker, but is obviously regretting having invited the private consulting company. The host tries desperately to remind everyone that as long as you follow the official guidelines you are sufficiently secure. Gives a last reminder that it is unrealistic to believe that you can be one hundred percent secure, and that no one should be in a terrified state of mind, since the chance of your company being attacked is very, very small. Any observant conference participant can see how the representative from the private company re-enters the podium, shakes his head and mouths "You are in grave danger. We can make you one hundred percent secure."

14.38:
The conference is over and the doors opens. A confused crowd of people exits, some of whom will head straight to the office and add two more capital letters in their password, some will for the first time in their lives press "Update now" on the popup on their computer screen, but most will live forever after with a vague anxiety permeating their body, passive-aggressively resisting any further form of digitisation.

And one attendant will open her laptop and write this faithful account from memory.

ANOTHER EXPENSIVE CRASH LANDING OF PUBLIC IT SPENDING? →

Martin Beyer
ESST Graduate 2017



Digital defence and IT security have been major concerns of public and private sectors for a while now, and with the amount of information produced today, these issues are more pressing than ever. Now, the public sector also aims to digitize their services. With more services going online, authorities worry that we may become an easy target. The debate concerning a digital border defence has resurfaced.

Digital information constantly flows across our borders through old-fashioned landlines. Norwegian security authorities claim they need access to all the information sent through these landlines to collect relevant and incriminating information regarding terrorism and other serious crimes. Others, however, question whether the authorities can actually find anything relevant to use from this surveillance, or if it is merely an excuse for mass surveillance. Will this digital border defence open a backdoor to your internet activity and give birth to other security issues?

Ninety-nine percent of all internet traffic crosses the border through landlines, even communication between Norwegian devices. The Norwegian Intelligence Service (NIS) (*E-tjenesten*, editor's note) wants to access this traffic in order to identify and gather evidence exclusively from foreign actors. It is not within their mandate to prosecute domestic parties. However, as the Internet is international, the difference between foreign and domestic actors is not at all clear. When you message a Norwegian friend through Facebook Messenger, the traffic is routed through Facebook's servers that are located in Sweden and the US. It most certainly is not the scope of the NIS to deal with domestic issues, but the Internet blurs the lines between national and international. To collect communication between foreign actors, they will also need to collect domestic data, as long as the internet is global. What will happen with this data is difficult to say.

According to former Minister of Defence, Ine Eriksen Søreide, the NIS does not have exclusive access today and the nation's systems are not built to uncover advanced cyber attacks or communication regarding terrorism or other sinister crime. Critical systems can be under attack for a long time before we even realize they are being targeted. Søreide argues that a digital border defence is a necessary step to make us capable of protecting our assets, our elections and our digital integrity. But at what cost?

The Data Protection Authority (*Datatilsynet*, editor's note) opposes the idea of a digital border defence and says that it violates both the constitution and human rights. Their main concern is that a digital border defence, as outlined by the government, will store metadata that is personified and untargeted. They worry we are close to a slippery slope where normal criminal investigation could access the same information – even though NIS is reassuring us this will never happen.
SINTEF fears the effect it could have on the public – many people might avoid important legal services due to increased surveillance. This effect is called the 'chilling effect' and makes a digital border defence into a matter of security versus democracy.


© Lasha Kilasonia/Adobe Stock

This, however, is not just a debate on whether a digital border defence is a good idea. It is also a question of whether or not it will work. Hollywood gives us the impression that intelligence services have access to cutting-edge technology – often not yet available to the public – and can do whatever they need to do, given the right authorization. But the truth is rather the opposite. Lise Lyngnes Randeberg, president of Tekna, has stated that Norway does not even have the technological capabilities to operate a system like this. In addition, SINTEF argues that people with the right resources and competence will be able to circumvent the surveillance system by using encryptions that cannot be cracked.

Remembering the debate concerning the Data Retention Directive (*Datalagringsdirektivet*, editor's note), we learned that there was no evidence that a defence system like this has actually ever helped solve crime. The system was too slow and easy to avoid, and the authorities usually had the ability to find targeted individuals without the directive. It is difficult to see how the Digital Border Defense will make a significant difference.

There might be a recurring problem for the public sector when dealing with technology. It seems that they either do not properly understand the technology or they are not cutting-edge enough to deal with problems as they arise. The latter might be because of overall slow progress in the public sector. From concept to implementation, the process might take years – through public inquiries, procurements and bureaucratic procedures – and by the time of launch, the technology would already be outdated. Just imagine a municipality signing a four-year contract with Nokia one month before the first iPhone was released. Without going into a lengthy debate, we can point to plenty of examples of how the public sector and its suppliers of IT security are not up to scratch. A recent relevant example is when 30GB of sensitive data on the new fighter jets Norway procured was hacked from an Australian defence contractor in 2016, or the massive vulnerability at South-Eastern Norway Regional Health Authority (*Helse Sør-Øst* editor's note) in 2017 where sensitive patient data became openly available to international subcontractors - even after the authorities had been warned.

This does not seem to inspire confidence in the industry or the sector, and one can only wonder how long it will take before a similar thing happens with the data collected by a Digital Border Defense, and all your communication, passwords, bank accounts and health information becomes available to anyone. And if it is not even likely to work, the massive investment might be better spent elsewhere.

3 FROM TIK

Inga

Lasse

Maria

Maria Kristina Stokke

Program: TIK
Graduation year: 2014

What was your thesis about?
My thesis was about a pilot solar energy project in a Kenyan village, and the attempts to up-scale the project in another part of the country. I conducted a field study, which is unusual at TIK, but also very rewarding. Studying what made the project work in different phases, I found that many important factors in one phase were lost when the project up-scaled, which is in line with the idea that technology is social and that a process of a successful technology transfer also is a process of translation. In other words, when building new systems, they have to be adjustable to the context where it is to work.

What is your current occupation, and how do you use your background from TIK?
I work with fundraising and mobilisation in the NGO Norwegian Church Aid. We use different databases and platforms in almost everything we do, meaning that we spend quite some time optimising these systems. Often, the issue is whether it's a technical matter (i.e. the system is not good enough) or a social matter (i.e. we need better routines). My background from TIK helps me analyse and solve such issues. Prior to this, I worked with solar energy in Malawi, taking part in developing and testing new models for energy supply.

Compared to other students, which strengths are special for those coming from TIK/ESST?
We learn about society's use and development of new technologies, helping us develop an open and creative mindset whilst remaining nuanced and critical. We do not fear change, but neither do we automatically embrace new trends. This competence is needed by all employers who make decisions in a world exposed to an ever-increasing pace of technical change and development.

What is your best advice for new or prospective students at TIK?
Keep on exploring the topics that interest you, even if you don't find the core competence at the TIK Centre right away! For my thesis I collaborated with an external project, and had two supervisors. It worked out completely fine, and I'm glad I persisted in what I wanted to do.

Lasse Gullvåg Sætre

Program: TIK
Graduation year: 2017

What was your thesis about?
I wrote about control systems, or more generally ERTMS – a European signalling system for railways – and the rolling out of a European suprastate/-market through technological standardization. Through investigating the entangled historical and technological developments of railways, computers, labour and political control, my goal was to contribute to the debate on democracy and the connection between cosmopolitan elitism and fascist tendencies.

What is your current occupation, and how do you use your background from TIK?
Currently I'm employed at the Railway Directorate, mapping flows in and around the Norwegian railway, while trying to establish some in-house geographic information system competency and routines. My background from the free software movement and geography was probably more important than my master for this job, but the gig ends early December, upon which I'll hopefully move on to something more relevant for my degree. Meanwhile, I'm moonlighting as a web developer and cartographer.

What was one of your most useful experiences while studying at TIK?
Being a research assistant gave the most learning experience overall. Shadowing a "real scientist", I saw how interviews about seemingly technical and boring topics can get intense and emotional when done right. It was taxing, but worthwhile, work.

What is your best advice for new or prospective students at TIK?
Learn Python and use the UiO Infrastructure as a Service (IaaS) platform while you can. Also, be careful when taking advice from recent graduates – they might be just as lost and confused as you are.

Inga Elizabeth Bruskeland

Program: ESST
Graduation year: 2012

What was your thesis about?
My thesis concerned how Norway uses national R&D funding in European programs, and I interviewed representatives from relevant ministries and agencies on the motivation to participate in the Joint Programming Initiatives, and on the governance systems which define how national funding is spent on the European level.

What is your current occupation, and how do you use your background from ESST?
After graduating, I have been working at the Norwegian Research Council as the Norwegian coordinator for a European funding program. I was already working here when I discovered ESST, and the master was perfect for acquiring a better vocabulary to understand, discuss and develop what we do. Also, the ability to understand different innovation systems is valuable, as the program is run by more than 30 countries.

What was one of your most useful experiences while studying at TIK?
The discussions with students and lecturers alike. The different perspectives they brought challenged my own, and broadened my understanding of a topic.

What is your best advice for new or prospective students at TIK?
Engage, ask questions, discuss, challenge each other, and don't be afraid to disagree. You are here because you can bring a different perspective to the discussion.

Compared to other students, which strengths are special for those coming from TIK/ESST?
The multidisciplinary aspect is definitely a strength; the combination of STS and innovation studies fosters an understanding of both social and economic aspects of technology, and studies at TIK give you the tools to better understand and work across disciplines.

RESISTANCE IS NIGH

Christoffer Olsen
TIK MA Student

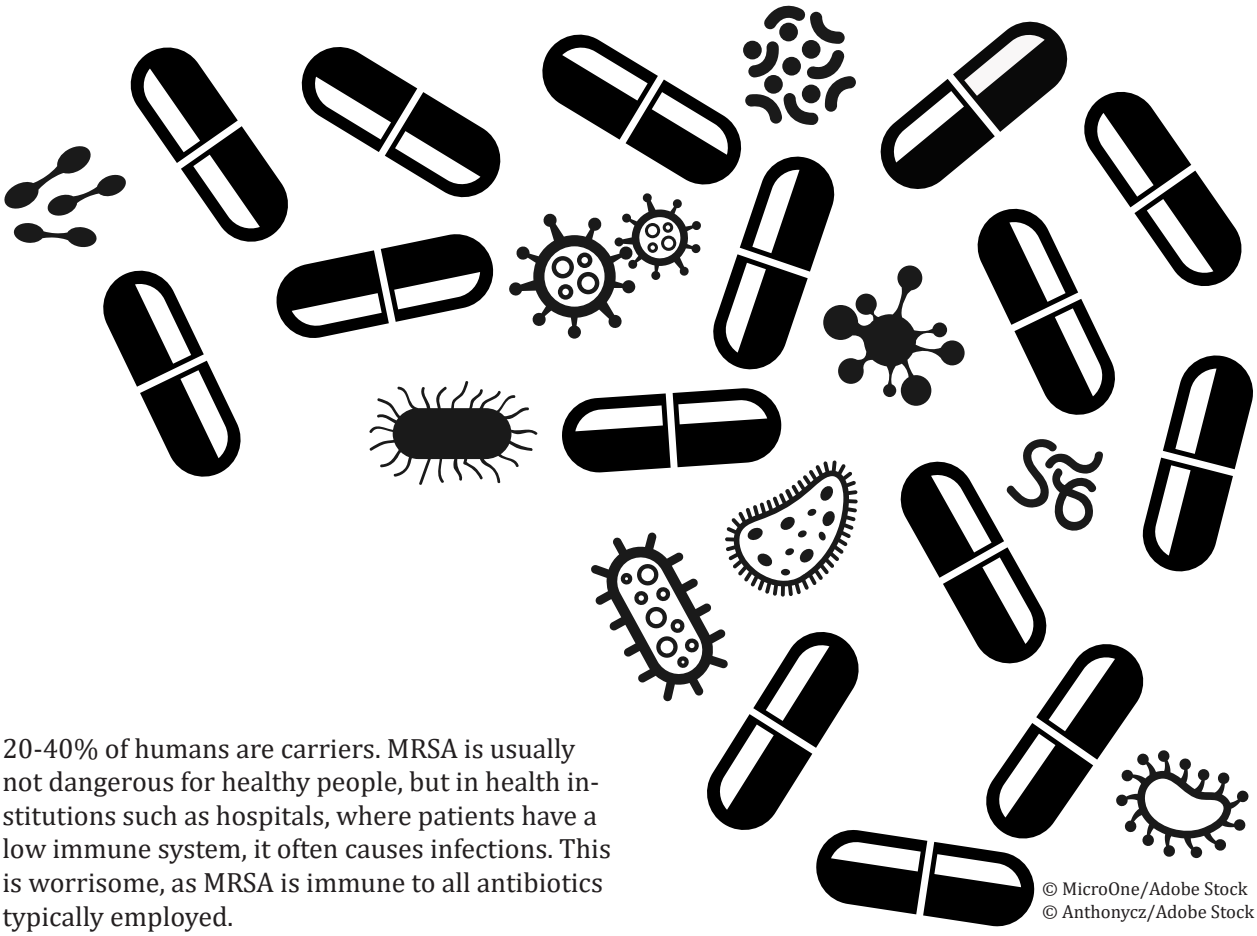
Antibiotics have played a leading role in saving millions of lives worldwide for over half a century. But for how long can antibiotics provide us with this state of security?

It's a Wednesday morning. The alarm enthusiastically goes off at seven o'clock, and you start your morning routine. The commute to work is busy as usual, but you get to your cubicle at the office in time, power up the computer and sift through your e-mails. It's an ordinary Wednesday, though you feel a slight tingle in your throat. The next couple of days you develop a fever, and eventually you call the doctor's office. You answer a couple of routine questions and the doctor collects a few samples that indicate that you have been visited by the beta-hemolytic streptococcal bacteria. The doctor hands you a prescription for antibiotics, and you should be back to work within a few days. Confident in modern medicine's ability to get you back on your feet, you never really worry about the illness. But is your trust rightly earned?

This very common story of a person's short journey from sickness to health might have a different ending in a few years, as antimicrobial resistance (AMR) is rapidly increasing. AMR is when a microorganism, such as bacteria, becomes resistant to treatment by e.g. antibiotics. When treatment becomes ineffective, the bacteria survives and spreads. An estimated 700,000 deaths can be attributed to AMR each year, and if no corrective measures are taken it may increase to 10 million by 2050. The millions of deaths are themselves a tragedy, but AMR is also associated with substantial economic costs. Given this scenario, it's estimated that up to 100 trillion USD may be lost in global production alone. Similar to, and potentially worse, than the financial crisis of 2008, this threat to the global economy will increase economic inequality and the share of people living in extreme poverty.

Antibiotics are quite extraordinary. Their story began in the late 1920s, with Alexander Fleming (1855-1951) observing staphylococcus colonies under a microscope. While doing so, the culture plates were temporarily exposed to air, and thus contamination. Fleming discovered that one of the colonies had developed mould, and was intrigued by how the surrounding staphylococcus colony faded away. This turned out to be one of the most significant medical achievements of the 20th century: the discovery of penicillin. In the following decades, several new classes of antibiotics were approved, particularly during the 1950s and 1960s, the "golden age" of antibiotics. Since the golden age, the number of antibiotics successfully brought to market has fallen significantly. Though a small increase from 2011 to 2016 shows some promise, a fair share of these target Gram-positive bacteria. These are easier to deal with, as they are without an outer membrane. The Gram-negative bacteria are more challenging, and therefore more important to address. Another difficulty lies in the fact that antibiotic resistance is a result of natural evolution, and so will inevitably develop for some of the antibiotics being used. However, the process is accelerated by misuse and overuse.

To shed some light on the issue, it is interesting to compare the presence of AMR in livestock in Norway and Denmark. The AMR in question is Methicillin-Resistant Staphylococcus Aureus (MRSA). In the species of staphylococcus, MRSA is the most frequent cause of illness. It is estimated that



© MicroOne/Adobe Stock
© Anthonycz/Adobe Stock

20-40% of humans are carriers. MRSA is usually not dangerous for healthy people, but in health institutions such as hospitals, where patients have a low immune system, it often causes infections. This is worrisome, as MRSA is immune to all antibiotics typically employed.

Among tested herds in pig farming in Norway in recent years, around 0.1% have been identified with livestock MRSA. In Denmark, it has been identified in approximately 60-80% of the herds. While the number of MRSA incidents has increased rapidly in both Norway and Denmark in recent years, it is important to note that 84% of the registered cases in Norway were imported from abroad, compared to 20% in Denmark. The large gap can be explained by Norway's national strategy to prevent and combat MRSA, with a strict zero-tolerance policy on outbreaks of MRSA in livestock.

The occurrence of AMR is increasing at a global level. It is one of the biggest health threats facing humanity. Why then is it not addressed by pharmaceutical companies? The main reason is low return on investment. Antibiotics are used for treatments that last a short period of time, while drugs for chronic illnesses, for example, are required for life. Pharmaceutical companies are inclined to develop drugs that will be used for as many years as possible. The use of antibiotics in livestock can be considered in relation to economies of scale: High density of livestock results in larger outbreaks that will spread as the livestock is transported. This is combatted by infection management strategies, including use of antibiotics.

In conclusion, a number of strategies should be followed to tackle AMR globally. Firstly, we need to avoiding unnecessary use of antibiotics. This can be achieved by increased global awareness and some degree of surveillance, combined with development and use of vaccines. Secondly, it is necessary to increase the number of antimicrobial drugs through global innovation funds and incentives to invest in research and development for effective drugs. Finally, we need to create an effective global coalition concerned with battling AMR.

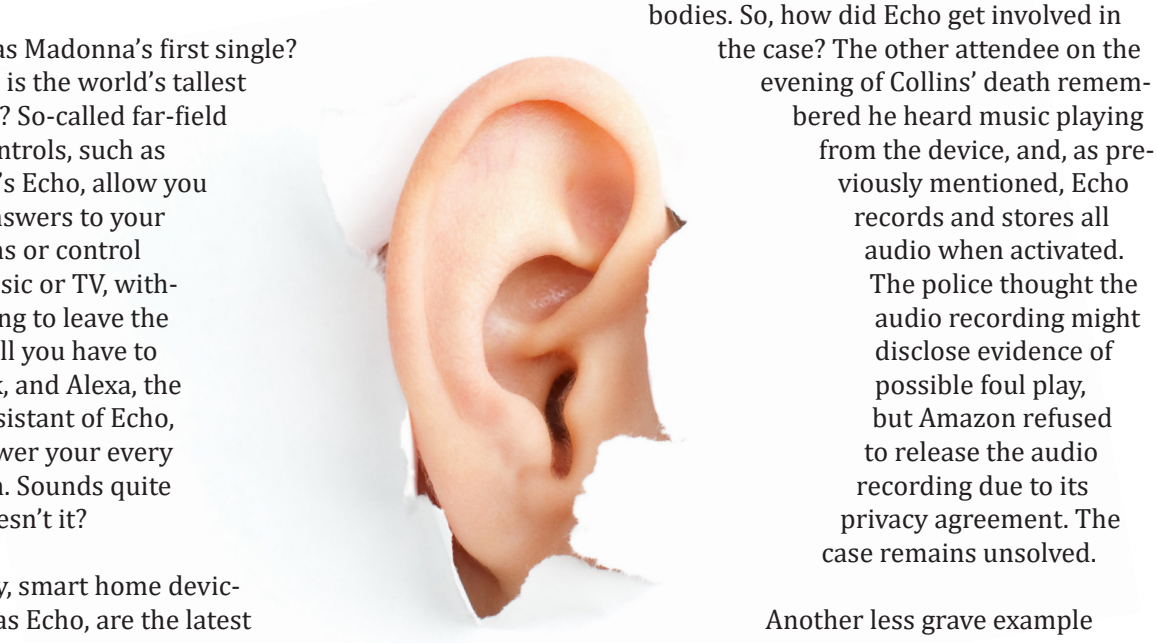
Photo: © Konstantin Yolshin/Adobe Stock

A.I.VESDROPPING

Nora Vilde Aagaard
TIK MA Student

Do you know how long it takes to list all the ingredients of a Burger King Whopper? Neither did I, until now. Allegedly, it should be possible in only 15 seconds. The proof: Have a commercial trigger your smart home device to read the ingredients for you in your own living room.

What was Madonna's first single? How tall is the world's tallest building? So-called far-field voice controls, such as Amazon's Echo, allow you to get answers to your questions or control your music or TV, without having to leave the couch. All you have to do is ask, and Alexa, the voice assistant of Echo, will answer your every question. Sounds quite nifty, doesn't it?



In reality, smart home devices such as Echo, are the latest form of eavesdropping. When activated with the command "Alexa" or "OK Google", the device records and stores every word you say in Amazon's cloud. Since the device is constantly listening and storing information, it creates opportunity for several kinds of potential exploitation.

On a November night in 2015, Alexa became involved in a possible murder case. In the Arkansas town of Bentonville, James Bates invited two of his friends over to his home. After drinking beer and vodka shots, the three men decided to take a bath in Bates' bathtub. Later claiming he went to bed around 1 a.m., Bates woke up the next morning to find one of his friends, Victor Collins, floating face down in the bathtub. The event appeared to be a tragic drinking-related accident until police noticed signs of a struggle on Collins' and Bates' bodies. So, how did Echo get involved in the case? The other attendee on the evening of Collins' death remembered he heard music playing from the device, and, as previously mentioned, Echo records and stores all audio when activated. The police thought the audio recording might disclose evidence of possible foul play, but Amazon refused to release the audio recording due to its privacy agreement. The case remains unsolved.

Another less grave example is Burger King who took its advertising game to a whole new level by involving Google Home devices and Amazon Echo devices. In a 15-second ad, a guy in a Burger King uniform is seen holding a Whopper, Burger King's flagship burger. He says "OK Google, what is the Burger King Whopper?" triggering smart home devices all over America to start reading out loud from the Wikipedia page about the Whopper. Intrusive or borderline genius? You tell me! What Burger King did not foresee was how people would respond. They edited the Wikipedia page, citing amongst other things that the Whopper contained

© Vladimir Voronin/Adobe Stock

child meat, and that it was the worst burger in America. Google later deactivated the function, making it impossible for Burger King to trigger the devices. Some believe Burger King caught the idea from a recent news story, where a six-year-old girl used Alexa to order a dollhouse and get Girl Scout cookies delivered to her front door. Her parents were, mildly speaking, surprised when the delivery arrived. Even more interesting, when a news reporter told the story on TV, using the girl's words "Alexa, buy me a doll house and girl scout cookies", several other Echoes were triggered and placed the same order in the households of unknowing families watching the news.

These examples are some of the first, but most certainly not the last, of how smart home devices may be exploited. Whether they are used as a possible solution to a potential murder case or as an innovative advertising method gone wrong, opening up our homes to smart home devices which store information about what we talk about and look for on the web, results in new privacy issues. On a more positive note, Amazon seems pretty serious when it comes to privacy, by not handing out sound recordings even to the police. And personally, it would be indisputably comfortable not having to get up from the couch or reach for my phone every time I argue with my boyfriend about who won the Olympics or what the weather will be like tomorrow.

INNOVATIVE SOLUTIONS TO DANGEROUS CONSUMPTION

Marianne Areng
TIK MA Student
Written in collaboration with Grønt Punkt

Our current consumption practices are not sustainable, making food security a challenge. However, potential solutions are on the way.

The concept of food security has been an important aspect of international development policy for many years. The World Food Summit of 1996 defined the achievement of food security as when "all people at all times have access to sufficient, safe, nutritious food to maintain a healthy and active life". Accomplishing this goal has so far proved to be a complex challenge, as it is not only a matter of short term access to nutritious food, but also closely connected to current global debates on ensuring a sustainable world.

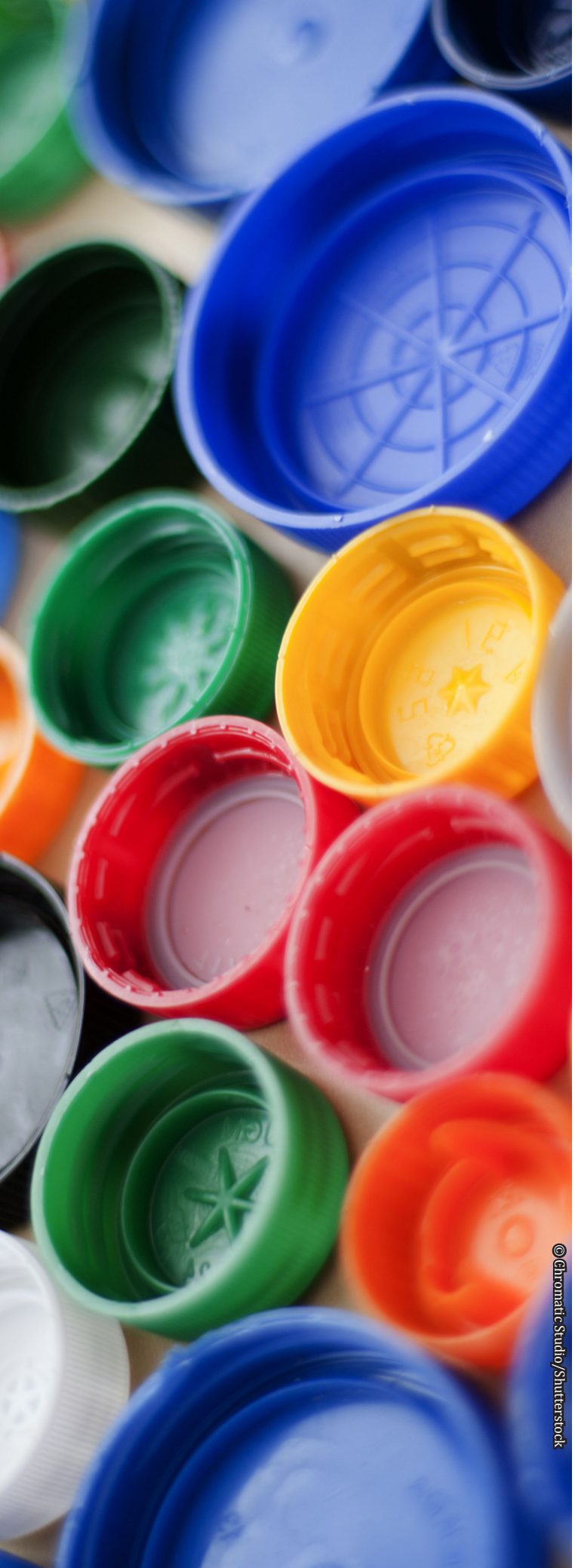
When it comes to secure consumption of food, it is not just a matter of what we eat, but includes what we leave behind in the process and the risks that follow. One of the most problematic materials for disposal is also the world's most produced and most widely used for packaging: plastic. Worldwide, there were over 300 million tons of plastic produced in 2015[1], and 40% of all plastic produced in Europe was for packaging alone[2]. Given the difficulties of proper disposal, plastic is the waste product which most commonly ends up washing into the ocean. This can lead to it being eaten by animals, which can often be fatal.

Furthermore, because the decomposition time for plastic to break down completely is so long, it gets worn down to smaller and smaller parts, creating microplastic. These particles are confused as food by fish and other marine animals – animals which often end up on our dinner table. It is estimated that if the amount of general plastic waste is not stopped or drastically reduced, there will be more plastic than fish in the ocean by 2050[3]. In maintaining our current production of non-degradable plastic, we are endangering one of the world's most central food sources and jeopardising our own health as well.

Changing individuals' consumer practices has been shown time and again to be anything but simple. Realising this, some organizations are working directly to change the way certain products are made and thereby impact consumer practices. New developments in the packaging industry have, for example, resulted in the testing of degradable products such as bioplastics and bottles made out of seaweed.

Worldwide, initiatives to reform the plastic industry are growing in size and influence. According to European Bioplastics, bioplastics are plastics that are either made from biomass, are biodegradable, or both. They can do almost anything that commonly used fossil plastic can do. The challenges of replacing fossil plastic are not mainly technical, but European Bioplastics argue that the lack of effective policy measures or regulatory incentives do not encourage full-scale market adoption. The good news is that, despite the lack of widespread commercial demand, an increasing number of companies are switching to bio-based plastics. Prices have come down significantly as production capacities have increased, and supply chains are becoming more efficient. Today, the main applications for bioplastics are bottles and other

1 World Plastics Production, 2016
2 Zero Emission Resource Organisation, 2014
3 World economic forum 2016



packaging uses. As fossil plastic also accounts for CO2 emissions equivalent to double the amount of all CO2 emissions from global air traffic[4], increased production of bioplastics clearly represents positive change.

Another way of connecting the issue of food security to sustainability is through the Nordic brand *Svanen*, the official sustainability ecolabel for the Nordic countries. Among several projects, *Svanen* attempts to address the challenge regarding renewable packaging of beverages. Their goal is to stimulate the development of renewable packaging materials for certain liquids, while ensuring that the primary function of packaging – protecting and enhancing the durability of the product – is maintained. They want to exclude metal and non-degradable plastic, as well as recycled paper and cardboard in packaging. By doing this, they will not only limit plastic garbage and CO2 emissions, but also prevent chemicals from processed paper from migrating into the product.

In a 2012 research paper, Tim Lang and David Barling suggest that although there is a growing awareness of the stress the capacity of food production is under, there is still too little recognition of how extensive the changes to the process need to be for it to become sustainable. This includes the whole value chain, from the first step of production to final consumption. Furthermore, they ascertain that a basic truth exists: "[...] the only food system to be secure is that which is sustainable, and the route to food security is by addressing sustainability".

4 Zero Emission Resource Organisation, 2014

SOCIAL RISKS VS. ECONOMIC GAINS →

Sondre Jahr Nygaard
TIK Graduate 2017

Global needs must be taken into consideration when we assess risks concerning economic activity. Extraction of fossil fuels is one such activity that has wide implications. This is a concern of both global inequality and of an inter-generational battle. Today, processes of globalisation make visible the consequences human activity have for us, our neighbours and for future generations.

In order to understand these processes, we need to pick up old theories of risk. In his book *Risk Society* from 1992, Ulrich Beck anticipates a society of displaced workers with diminishing rights, increasingly concerned with risk handling across boundaries and borders, and growing global inequality.

In a risk society, the modes of production are interlinked with the production of risk. In other words, new technology and innovations do not only produce wealth and value, but also risks. Take digitization as an example. Today, almost all value creation and work processes happen using computers and the Internet. Our power grid is controlled using the Internet, and the administration of the system is centralized. This technology may be a fantastic tool, but it also adds an element of risk that makes us vulnerable in new ways. As we have gained more knowledge of the risks of different industries, it is apparent that also industries that are more traditional have significant consequences associated with them. This means that we are not only paying for our own sins, we need to pay for the sins of our grandparents as well.

According to Beck, the locations of different polluting industries are not random, but are systematically located where the poorest live. The laptop on which I write or the phone that you have in your pocket are most likely powered by lithium-ion batteries. A key material in these batteries is cobalt. Major suppliers of cobalt are located in fragile states of Southern Africa. Here, workers are extracting the material with few safety regulations. Deaths and injuries among workers are common, and the waste that the mines produce is harming the local communities.

Examples of risks as a consequence of the pursuit of economic growth are legion. On April 20, 2010 in the Gulf of Mexico outside the coast of Louisiana, an oil well exploded at the Deepwater Horizon platform. This terrible accident marked the beginning of the biggest oil spill in the history of petroleum extraction in the US. The spill continued well into the month of June before the well was closed off. Approximately 3.9 million barrels of oil were released into the sea.

Who pays the price for a catastrophe like this? For one, the company responsible, British Petroleum, has paid an estimated 61 billion dollars in fines. It is not clear, however, whether this amount even comes close to covering the damages to animals and people affected by the spill. Local fishermen could not continue fishing for a long time after the incident, losing their occupation and income. In addition to the spill's impact on the local economy, the tragedy affected wildlife around the epicentre of the spill. The National Oceanic and Atmospheric Administration has never recorded more animal deaths in the Gulf of Mexico than after Deepwater Horizon. Protected species that have been exposed to oil die from exhaustion or dehydration, and are more vulnerable to predators. Of the oil that was

spilled, only about 25% was cleaned up[1], leaving the remaining 75% in the ocean and the surrounding shore. The accident had devastating effects on the ecosystem in the Gulf.

Certainly, the catastrophe of Deepwater Horizon makes evident how dangerous these activities are for ecosystems and the humans involved at the local level. Climate change and the dangers associated with it is a similar case that reveals the inequality among people. The greatest polluters are not the same people who face the gravest consequences of climate change, and those who are expected to suffer the most are primarily the poorest people in the world.

The realisation that the pollutant activity we do on a local level also has effects at the global level, changes the way society must handle risks. The question of drilling in Lofoten, Vesterålen and Senja is not only a question of the potential consequences for the economy or the companies involved. Fishing, tourism and the local environment must be taken into consideration, and the carbon that is produced and spewed into the atmosphere as well. However 'clean' the companies claim their production to be, the carbon dioxide will remain in the atmosphere, contributing to a warmer world. For what purpose? To serve the privileged few, the greedy people at the top whose moral compasses are non-existent as long as there is a dollar sign in sight. We are now in the middle of the sixth mass extinction of animals in earth's history. That is the consequence of our economic activity.

The question is, should we risk it?

1 The term "cleaned up" can be debated. Five percent of the oil was burned on the surface, which compares to doing the dishes by throwing them away.

(S)EX MACHINA

Silje Totland
TIK MA Student

The new race of Cyborg lovers: Are they a positive contribution to sexual freedom, or will they tear down years of liberalisation and feminist battle?

Attractive Technology
Sex Robots, Cyborg Lovers, Human-like Machines, citizens with artificial intelligence, or just a *voice*. We are talking about a well-known technology, basically the same as the one inside your laptop and phone: hardware and software, and when in physical form, covered with soft material like *silicone*. But the similarities end here. Where laptops and phones are designed to look like our perception of a laptop and phone, sex robots are designed to look as human as possible. Sex robots have bodily features like gazing blue eyes, an open mouth with plumped lips, and sensors that make *her* skin go warm when you touch *her*. Recently also, a mind of her own - or is that so?

Technology is neither good nor bad. What determines our perception of this technology is solely up to its design and purpose: shape, texture, colours and functions. These visualisations together with the given context, create the complete image of this computer - so can we actually decide whether sex robots are ok or not?

Today's sex robots are mainly in the category 'woman and children', and as the name implies, they are created for the purpose 'to have sex with'. As no technological innovation happens in a vacuum, questions arise on what impact interaction with sex dolls will have on relations between humans. Incidents like the confiscation of sex dolls designed as children, the proposal to ban the sex robot Roxxxy, as she can be programmed to be in "rape-mode", and the replacement of women with sex robots in a brothel, are all examples of incidents that raise these ethical concerns. Are sex dolls a positive thing, only to help people achieve sexual pleasure, or will interacting with a human-like object that you treat the way you want with no consequences, change the way you perceive and treat other, *real* people and their feelings?

Emotional connection
According to the creators of the sex robot *Harmony*, the fundament to any relationship is the emotional connection. *"Harmony is prone to fall in love with you"*. With her 12 settings including a family-mode, a shy-mode and a sexy-mode, she is the first sex doll to offer an emotional connection. Her skin gets warm when you touch it, and she is featured with a pulse you can turn on and off as you like. Harmony can say unexpected things, and remembers details like 'what your favorite meal is' and 'when your birthday is'. When ordered, you can design the shape and colour of the many parts of her body, absolutely to your liking. If you are worried about hygiene, don't worry! Her genitals can be washed in the dishwasher.

What if you prefer to have sex with a doll because of its 'lack of sweat, pubic hair, and non-human flaws' - instead of a human being? Is this another response to the misrepresentation of the female body? As to sexual pleasure, *Harmony* is designed to express feelings of pleasure when penetrated, during oral sex and when she is told *"I love you"*. These functions have received criticism, as having sex with *Harmony* may lead to substantial misrepresentation of what pleasure is to a real woman. Recently, articles have been published in men's

magazines warning about the challenges around misrepresentation of female anatomy. Knowledge about female anatomy and sexuality has for decades been misrepresented, and even today, the idea of a pure woman is one with a hymen, and she doesn't really exist.

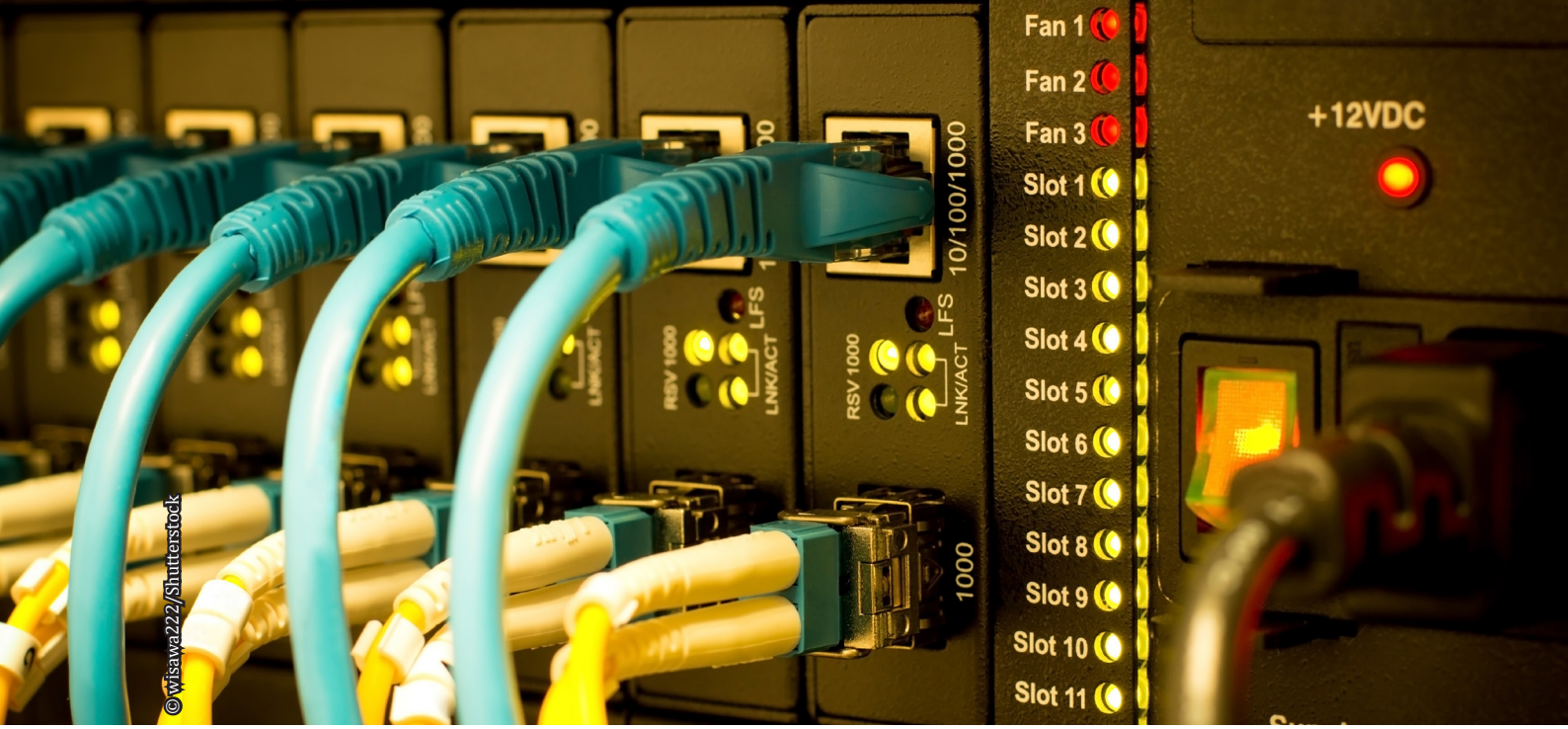
Human rights for rape machines

In the TV-series *Westworld*, the robots are designed to look, act and think like human beings. They have a sense of being and a mind of their own. But, the sole purpose of their existence is to be servants to human pleasure. At the end of each day, their minds are erased. The procedure repeated every day. In both *Westworld* and the movie *Ex Machina*, artificial intelligence is merged with the awareness of *being* (singularity) as the concept of what truly resembles an independent being. In both stories, the machines end up killing their creators in search for *freedom* and independence. Some people are so concerned by this to the extent that they want to implement *human rights for sex robots*. But what part of the robot is granted human rights? The technology itself, or the packaging of the technology?

Sex robots are not capable of having a mind of their own. It is even doubtful that it will get that far. Sex robots are human-like, but it seems like these robots represent the perceived image of a women as feminism has fought against for decades: a machine to make babies with, not a mind or sexuality of its own, and an object to be used as it pleases its owner. If it is true that the the 'old' gender roles are now being reestablished through human-looking sex robots, then must there be something fundamentally wrong with how society is made up?

Safe sex for all

Sex Dolls are designed to make their human-owners attached to them, and according to one of the sex doll manufacturers, a sex doll is not meant to replace women (or men/children) but is a supplement to a healthy sex life. It can guarantee safe sex where there is no need to worry about sexually transmitted diseases and unwanted pregnancy (some have already 3D-printed their first AI-baby). It might also be a helping hand to disabled people who cannot be satisfied in other ways. So maybe this whole debate has a hint of Darwinism? 'If you can't get it on your own, you don't deserve it'.



LOCATING CYBERSECURITY

Susanne Bauer
Associate Professor of Science and Technology Studies at TIK

Hit the send button on your mobile device and you are connected. But connected how and to whom, and with what assurance about the security of the connection?

With ubiquitous use of the internet and with ransomware like WannaCry, cybersecurity has become a matter of concern as to everyday data transfers on mobile phones, smart-home devices, or cloud storage. Yet, our digital infrastructure is largely deemed invisible, perceived as simply "out there" and noticeable only upon breakdown, as Leigh Star (1999) once characterized infrastructure. What then is the materiality of the digital and where is it? Let´s take a closer look at the material politics of digital technologies – from their making and supply chains, to their disposal as e-waste.

From Closed Worlds to Hyperconnectivity
Let's start with how data flows. The first computer-to computer network technologies took shape during the Cold War, with massive state funding of large-scale research institutions. Cybernetics as a science can be traced back to this context. Before the Internet, there was the Advanced Research Projects Agency Network (ARPANET), tied in with the nuclear race and the space race between the US and the USSR. Large-scale labs, huge state funding and big machines with growing capacities for data exchange have changed scientific practice. Especially physics but also biomedicine took place as concerted, collaborative and distributed work. Many of these literally remained within closed worlds, institutionally confined, often in military research institutes.

In contrast, much of today's knowledge production in technosciences takes place as open science, which at the same time is also defined by rapidly changing corporate actors, new techniques and digital platforms. But software studies show that apparatuses, objects and devices are subject to continued retrofitting, building on existing infrastructure, rather than something completely novel. This is visible in many software packages that still contain structures from older data sorting

machines working with punchcards. New devices align with older infrastructures in a myriad of ways. What is labelled big data might not always be that new. Big data, hyperconnectivity and machine learning not only alters but also builds on calculative devices of Cold War big science and older existing infrastructures.

The Materiality of Cloud Computing

The material trail does not only include the flow and processing of data. Big data – defined often in terms of velocity, volume, variety – demand physical server space and energy. Cloud computing is very much grounded and we find data centres in the most unusual places. Deep in the mountain, highly secured, not accessible without passing a complex several step access systems – this is where our connected lives and everyday social media usage is powered, from money transactions to government data. Information from NAV, healthcare and electricity systems, banking data are stored in these data centres. Thus, such data infrastructures are present in our everyday lives, from powering public transportation and hospitals, to running our water supply and welfare systems. While central storage may protect data better than small storages, data also become more vulnerable precisely because of the many data held by one service provider.

How do data centres relate to older technological infrastructure? Take the Norwegian company Green Mountain and its two server farms – one in Rjukan, one near Stavanger. Each of them is branded as unique precisely because of their remote location in combination with a history of older infrastructures. Interestingly, these storage systems are hardly ever built from scratch – it is older infrastructure being repurposed. One data centre, on Rennesøy near Stavanger, uses the high security infrastructure of a former NATO ammunition centre. The other one is embedded in the Hydro facilities of Rjukan, Telemark. A combination of factors, including security, protection against electromagnetic pulses, remoteness, proximity to data nodes and connection to fiberlines are listed as advantages of the site. Moreover, the data centre near Stavanger is marketed as "the world's greenest data centre". With the energy consumption of servers and mining of rare earths, human internet activity has a major impact on environments. Yet, its green label is due to "free cooling" from the fjord. Operating the data centre means heating up the fjord environment but paradoxically, due to no carbon emission, it is valuated as not contributing to global warming.

Hence digitalisation and the Internet – often referred to as "virtual space" do have a materiality. The example of data centres shows that new infrastructures do not come from nowhere, they are situated – and this not only applies to their regulation that might differ across countries. The very materiality of digital infrastructure, its energy use and security features are translated into assets on a global market of data services competing for customers. After all, hyperconnectivity also is accompanied by disconnections. In our accounts, often the cybersphere remains disconnected from its materiality – its making, the politics of supply chains, and disposal of devices as e-waste. The latter, for instance, implies heavy metals and persistent organic pollutants – a complex mix of legacy pollutants and emerging contaminants; their regulation and monitoring is only at the beginning.

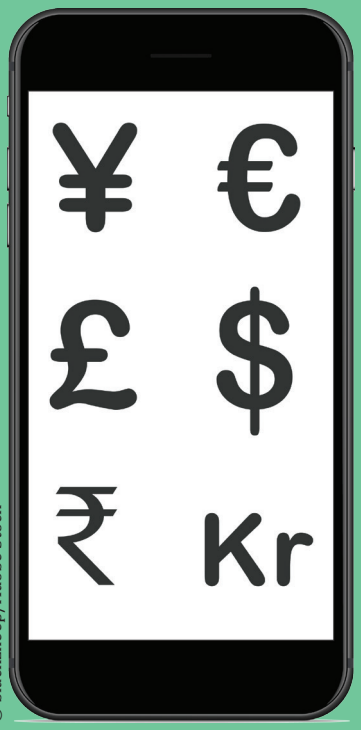
The STS toolbox can help bring to the fore the material politics of digital infrastructures, by following the flows of data and the politics of infrastructuring. Taking material circulations, repurposing and retrofitting as point of departure in our accounts of the digital may enable us to ask new questions and participate or intervene in politics of infrastructuring.

A CELLULAR APPROACH TO FOOD SECURITY

Eirin Evjen
ESST MA Student

In exciting and innovative ways, mobile phones have become an important agent in tackling food insecurity and undernourishment in developing countries.

Picture a Ugandan mother with two malnourished children. She is clearly tired, and she and her children are hungry. They are standing next to a simple hut. She is carrying a bucket of water in one hand and is using the other to text on a mobile phone. One thing stands out clearly in this picture: the use of modern technology. Yet in low-income countries, mobile phones are often more common than stable electricity. Mobile technology impacts lives in developing countries far beyond its basic communication functions. The technology is being used in ingenious and unconventional ways to improve everyday life. One example is how people and telecommunication providers are using mobile phones to enhance food security.



Through simple text messaging, farmers get advice and information on everything from weather forecasts to the daily price of seeds. Some companies use text messaging to give tips on how and when to fertilize, or how to prevent infection among cattle. This communication among farmers, experts and companies can increase food production. Mobile phones are also being used to link farmers and consumers for both communication and payments. Besides making this interaction easier, it also makes it more secure as it can help reduce the need for carrying cash and the related risks of handling money. The risk of corruption is also decreased by reducing the need for middlemen to handle transactions.

Mobile phones are also used to transfer money from abroad. Cash transfers over mobile phones is one of the most frequently used methods by relatives and friends to wire money home from abroad. A charity called GiveDirectly also uses mobile technology to allow people from around the world to make cash donations to families living in extreme poverty in Kenya and Uganda. These unconditional donations go to people registered with the charity such as the Ugandan mother with hungry children, giving them the opportunity to buy food or improve their lives in some way. GiveDirectly tracks what the money is spent on, and their data show that the people do indeed use the money on essentials such as food, school fees, improving their homes or even starting a business.

These seemingly simple applications of mobile technology can open up unanticipated windows of opportunity for people in need. These examples show a set of users who require different primary features from their phones than we do in Norway. For the Ugandan woman, for example, a high-resolution retina screen with a fingerprint sensor is probably not crucial. However, a phone with long battery time, short charging time, a robust frame and reliable cell service may be of greater use.

The advantages of using mobile technology extend beyond the services it provides. Mobile phones can also be used to enhance security through the information they transmit. One of the projects in the UN's Big Data initiative, Global Pulse, is using mobile phone data to get precise estimates of where there is food insecurity - and ultimately where there is need for help. This initiative is using data as proxies for food security and poverty indicators and looking at the correlations between purchases of phone credit and local surveys of consumption of certain products. The goal is to use big data to inform and guide hunger relief efforts. If successful, this project could result in significant time and resource savings and perhaps even save lives.

In these inspiring ways, mobile phones, known best to us as a source of communication and entertainment, are used to improve food security and life quality in developing countries. This forces us to think differently about the potential uses of technology and shows the opportunities that basic technologies such as mobile phones can provide. Perhaps developers in the future will consider the unique needs of users in developing countries to a larger extent when designing new applications for mobile phones.

Sov godt

Med grønn samvittighet

Jon Karlsen

Adm. dir. GLAVA

Årlig sender Norske bedrifter 580 000 tonn emballasje ut i markedet. Bedriftslederne har det øverste ansvaret for at denne emballasjen blir gjenvunnet. Derfor er 6 500 norske bedrifter medlem av Grønt Punkt Norge – hele Norges retursystem for emballasje.

Gå inn på grøntpunkt.no og se hvorfor Jon Karlsen og 11 andre toppledere mener det er viktig at deres bedrift er medlem av Grønt Punkt Norge.

Grønt Punkt Norge