THUTO KE THEBE

UNIVERSITY of BOTSWANA FOUNDATION

The 2019 DLIS 3rd Biennial Conference

Information and Knowledge Management: Towards the Attainment of Sustainable Development Goals and Knowledge-based Economy

Proceedings of the DLIS 2019 International Conference

Hosted by the Department of Library and Information Studies (DLIS)

15th - 17th April, 2019

At the University of Botswana, Conference Centre, Gaborone

Editors: Prof. P. Jain, Prof. N. M. Mnjama,
Prof. O. Oladokun & Prof. K. H. Moahi

Published by:
Department of Library and Information Studies
University of Botswana
Private Bag 00703
Gaborone Botswana

ISBN: 978-99968-458-7-1

PART SIX

EDUCATION & CONTINUING PROFESSIONAL DEVELOPMENT

THE NORDFRONT CUSTOMER DATABASE-LEAK: A CASE STUDY

Rikard Friberg von Sydow
Södertörn University
Email: rikard.friberg.von.sydow@sh.se

Abstract
In June 2017 the Nordic National Socialist organization "Nordic Resistance Movement" discovered that their web-shop, "Nordfront", had been hacked and the customer data leaked on the Internet. Later they admitted publicly to being hacked and soon thereafter the actual data base was released by the perpetrators. Online discussions and media reports followed. Politicians who had ordered merchandise from the web-shop had to resign and musicians who had done the same had their concerts canceled. Data hacking led to a political and cultural scandal in Sweden with consequences for those involved. The purpose of this study is to investigate the reactions in online forums from persons in the political sphere that was affected by the leak. How do commentators react when information that connects a person to a controversial, and in this case anti-democratic and racist, political organization, is spread on the Internet? How is the quality of the information valued from an information security perspective? How can the database-leak be analyzed with help from models of information security? The study will be done using a case study method, with the main focus towards the supporters of the Nordic Resistance Movement.

INTRODUCTION

In June 2017 the Nordic National Socialist organization "Nordic Resistance Movement" discovered that their web-shop, "Nordfront", had been hacked and the customer data leaked on the Internet. Later during the summer they admitted to being hacked and soon thereafter the actual data base was released by the perpetrators. Online discussions and media reports followed. Politicians who had ordered merchandise from the web-shop had to resign and musicians who had done the same had their concerts canceled. Data hacking led to a political and cultural scandal in Sweden with consequences for those involved.

The purpose of this study is to investigate the reactions in different Internet forums and media reports regarding this leak. How do political supporters and non-supporters react when information that connects a person to a controversial, and in this case anti-democratic and racist, political organization is spread on the Internet? How is the information valued by media and the public from a source critical and information security perspective? How can the database-leak be analyzed with help from models of information security?

which time during that day the order was placed. Customer IP is the internet protocol address from which the customer placed the order. This does not need to be the customers home internet protocol address, the unique address is just the network to which the customer was connected to when ordering.

All columns beginning with "Billing" and "Shipping" are connected to the physical addresses to which the bill was sent, and to which the ordered items was sent to. In most cases these addresses are the same. "Shipping Country" is the country in its standardized abbreviation. SE for Sweden is the most common and NO for Norway is quite common in the customer database. There are also orders from Denmark (DK), Finland (FI), Germany (DE), France (FR) and Russia (RU).

The last category "Order items" describes the item/items the person ordered (books, propaganda material, t-shirts, flags and banners et cetera). Unfortunately this category is not present in the database until 2015, and there are no evidence of how this information was communicated earlier (2012-2015). The information – which must have been communicated in some way or other – might have been stored in another file during this time. Maybe the web-shop generating the customer data changed that year, and the original (pre 2015) database was exported to the new web-shop. But this is just speculations. At least we can be certain that something changed in 2015.

The customer database file consist of about 5000 rows, each corresponding to an order (from the web-store). The oldest order in the file is from 2012 and the latest from 2016. Some people have ordered more than one time during these years, so the customer database does not consist of 5000 people, but an amount lower than that (No Front Friday customer database 2017).

REACTIONS TO THE LEAK OUTSIDE THE NORDFRONT-SPHERE

First the discourse in which the leak appeared will be described. This will be done by describing reactions to the leak outside what could be called the "Nordfront-Sphere", the "Nordfront-Sphere" being members of the Nordic Resistance Movement and their supporters. A discussion in a Swedish public internet forum, Flashback.org, and articles in the news media about the leak will also be used to describe (and construct) this discourse.

Flashback forum is an open, free-speech, internet forum. It is a common meeting ground for persons within a wide area of political opinions, with a focus on the political extremes. Researchers have been using Flashback as a source to find discussions regarding subjects related to drug use, (Månsson 2014, Andreasson & Johansson 2016), racist opinions (Malmqvist 2015) and online suicides (Westerlund et al 2015). Subjects discussed on the Flashback forums are often controversial and the members are generally anonymous.

Within 24 hours, a Flashback-user created a discussion-thread ("The Nordfront customer register is out") regarding the leak (Flashback 2017). The opinions on the Flashback forum might help us understand the reactions from posters in the Nordfront comment section that will be analysed later. A brief survey of the opinions on the Flashback forum will be given. The comments in the forum will be splitted into two areas – negative comments (negative towards the leak) and positive comments (positive towards the leak). The survey will take higher notice to comments that could be considered typical (stated by more than one user) or paradigmatic (stating an opinion that changes the subject). The forum thread consists of around 140 comments and only a few of these will be reviewed.

Among the negative comments we find such statements as "I wonder if my name is in the registry (I am a supportive member). I am not surprised that they lack IT-security – this might be what sends the organization to its grave" (the user "Adolf512"). Or a post stating that "If they lack in security in this way they could have given this list to the Secret police right away instead. The person responsible should be thrown out of the organization" (the user "Jeffrey. L Dahmer"). These statements are generally critical towards the lack of energy that the organizaton had used to sustain information security. You could call this a disappointment with the level of implemented IT-security.

Positive comments are generally very few. As it seems very few persons that are happy that the leak occurred because they are political opponents to the organization seems to have posted. Or – which always is a possible when you investigate material created by users on internet forums – their comments have been deleted by the forum moderators. One kind of comment that will be classified as positive are quite common: the fatalistic kind. They are stated by users who support

the organization but don't think that the leak will affect the organizations struggle in any way. Or that the leak might even strengthen the "fight for the cause". One such opinion is stated by the user "Sperrsson" who writes that "this (the customer database) is a list of good Swedes that seems to love Sweden and are willing to fight for the people." This kind of comment might be a way of sending support to persons affected by the leak and the message that they should not be ashamed of their opinions.

The leak had some news media impact. Some media coverage will be shown here trying to choose t the media sources that reveals the most information. Generally this media is center or left-wing politically and this is of course good to keep in mind in this case. The left wing magazine ETC publishes several investigative articles considering the leak. Revealing that politicians from the right-wing party "Sverigedemokraterna" and musicians from the Swedish Black Metal band Marduk are among the customers (ETC 2017). The liberal newspaper "Expressen" revealed that a politician from the christian democratic party "Kristdemokraterna" resigned because of the leak, being revealed as a customer in the database (Expressen 2017). The Swedish web-page "E-handel" who caters to entrepreneurs in online shopping and E-business writes a conclusive article discussing the consequences of the leak and citing other media that has published articles regarding it (E-handel 2017).

METHOD AND RESEARCH QUESTIONS

This is a case study. The information used is derived from a single case (a database leak) using several different sources. Using case study as a method the purpose is to study a particular event within a context (Pickard 2013, p. 101). It is a case study that emanate from questions central to my subject, Archival Science. Thomassen defines Archival Science as being distinct in its research object which is both information itself and the processes that have generated it (Thomassen 2001, p. 382). Both these research object will be central in this article, the process starting when the information leaks from the closed server to the open internet. If we would use the Record Continuum Model, first presented by the Australian archival theorist Frank Upward, the database leak would relate to the part of the continuum called "Pluralize" in which an information entity is spread from an organization (and its corporate/individual memory) to the collective memory realm of the Internet (Upward & McKemmish 2006, p. 225). The Record

Continuum Model will not be used in this article, but the model, in a modified way, might be an interesting tool for further investigations of database leaks from an Archival Science perspective.

The reason to examine this leak is to understand how doxing is used discussed in connection to a not generally accepted political ideology as National Socialism. To do this three research questions have been constructed. These research questions are connected to different actors and agents in the leak, the perpetrators (the hackers), the doxed individuals and their supporters (the "Nordfront Sphere"). The last question will try to answer questions regarding the quality of the information.

RESEARCH QUESTIONS

R1: What are the motivations of the perpetrators? Do the motivations correlate with the descriptions of doxing we find in Douglas description? Which of the variants of doxing is closest to their description of their motives?

R2: Which are the main reactions to the leak in the comment section of the Nordfront website (anger, satisfaction et cetera)? Who expresses these reactions? What motivates these reactions?

R3: How is the quality of the leaked information discussed? Which terms are used and what kind of information is considered desirable in the context of doxing?

Using these questions as an analytical tool while looking for the answers in the chosen material will give us new insight both regarding doxing in general and regarding this case in particular.

DOXING – AN EXPLANATION OF AN INTERNET PHENOMENA

In "Doxing: A Conceptual Analysis" Douglas "suggest that doxing should be understood as releasing publically a type of identity knowledge about an individual (the subject of doxing) that establishes a verifiable connection between it and another type (or types) of identity knowledge about that person" (Douglas 2016 p. 3). This suggestion is grounded on the internet phenomena of "handles" - that a person uses one name on the internet and another in life outside of internet (Douglas 2016 p. 3). The customer database-leak that is analyzed here is not in perfect relation to this, but the two phenomena still bear enough resemblance. I would argue that a large quantity of the customers present in the database tries to keep a closed border between their personal life

with work, relations and recreational activities and their political life with the support of a movement that is not considered a part of the accepted political landscape. It is the connection between these two parts of the customers life that is at stake when the database is released.

According to Douglas description there are three types of doxing: Deanonymizing doxing – in which the connections between a pseudonym and an actual identity is revealed. Targeting doxing – in which the physical locality and other information that helps locating a person is released. Delegitimazing doxing in which compromising information about a person is spread. Douglas main example here is when nude pictures of a person is spread – an activity to delegitimize a person often referred to as "revenge porn" (Douglas 2016 p. 5ff). In this case the two later types, Targeting and Delegitimazing doxing seems at the first glance to be close to the description of the leak. These two types are, according to Douglas, often seen together in a way that in many cases makes it hard to tell them a part (Douglas 2016, p. 8). To target someone you need to be delegitimazing (why would you otherwise target them?) and to delegitimize someone you need to know who they are (thus targeting them).

Why is doxing so effective in the age of the internet? One way of describing this is to turn to Marshall McLuhan classic work "Understanding Media" where the famous line "The medium is the message" was first coined (McLuhan 2005, p. 11). To describe the internet you could paraphrase this line and suggest that "the possibilities of the medium is the message". Internets power of spreading a message using bandwith never seen before in any medium makes it possible to use as a threat towards a person. And in the case of doxing it is the possibility to spread information that is in focus – not the quality of the information itself. This makes it very effective as a tool for delegimization. Returning to McLuhan it is not the first time a medium of communication changes the rules of a game, McLuhan uses the example of an arrest of a criminal in the 19th century that was possible due to the new communication tool – the telegraph. It is clear that different tools of communication are different in their effectivity in reaching a certain goal. The power of the telegraph, with its possibilities to send an arrest order between two cities faster than a train, scared the 19th century criminal. In the same way the internet, with its power to spread information, scares a person who wants to hide his or her political identity or other sensitive personal information. Doxing of national socialists is not a new phenomena in

Europe and North America. It has been done multiple times before and is considered to be an effective tool by their proponents. One of the reason being that it makes them afraid to state their opinions (VICE 2017).

THE ATTACK AND THE ATTACKERS

The persons hacking the server and stealing the customer database called their attack "No Front Friday" and themselves "The 1337 Antifa hackers" (No Front Friday release letter 1, 2017). The numbers 1337 is hacker slang for "Elite" (Urban dictionary 2018). After the release of the customer database, the hacker group released more information gained through hacking the Nordfront-server (comment section registrations, passwords et cetera). The releases were done through the groups Twitter-account (No Front Friday Twitter Account 2017). But only their first release, the customer data base, will be used in this article.

In the release letter there are some thoughts from the hackers regarding both the customers and the Nordfront-members managing the customer database. Their statement will be used to answer the first research question regarding the motivations of the perpetrators and how this motivation correlates with the descriptions and definitions of doxing that has been described above.

"The 1337 Antifa hackers" are very open with what they consider to be their purpose with leaking the customer database. They state that:

> "So, why are we dumping the customer data from the nordfront store? It's very simple actually, we don't have any hidden agenda. We want to damage NRMs organization, plain and simple. Every purchase from the site enables the crazy nazi cult to organize demonstrations, print stickers and buy weed. We can't have that." (No Front Friday release letter 1, 2017)

The main focus here is not to hurt the customers – but to damage the organization. The purchases from the web-shop supports the organization, thus contributes to its action. Here, in the beginning of the statement the customers are just described as collateral damage in a political struggle. This changes further on in the perpetrators text.

> "But I only bought a book" some customers will predictably whine, "Isn't there freedom of expression and freedom of thought?!". BU-f*cking-HU. You didn't JUST buy a book, you sent your money to the 9-fingered, bomb building, knife waving nazis that repeatedly hurt and kill immigrants, LGBT persons and political opponents. By "just" buying a book you are complicit in their crimes. Suck it up." (No Front Friday release letter 1, 2017)

The continuation puts more focus on the actual customer in the database, claiming that they "did not just buy a book", they supported murderers. This makes, according to the perpetrators, the customers complicit in these crimes.

> "The NF store does not consider your security, neither do they inform their customers about past breaches. Instead they lie all the way back to the bank." (No Front Friday release letter 1, 2017)

Here, the hackers seems to want to turn the customers against the Nordfront web-shop. They did not consider your safety as they should have done. This argumentation that seem to try to create a divide between the Nordfront web-shop and its customers continues, now with the focus of the doxing of the customers.

> "The next time you find yourself wanting a fifth copy of the Turner Diaries to jerk off to, take a second to reflect. Do you really want to show up in a dump like this again? What will your employer say when they google you? How about your next employer or your land lord, or your neighbors? In the end, thinking rationally, you will come to the conclusion that you are better of getting your books from another store." (No Front Friday release letter 1, 2017)

This is what we would call a threat of further delegitimatizing doxing, the type of doxing that Douglas describes as "in which compromising information about a person is spread". If "employers, landlords and neighbors" find out what kind of political organization the customer supports – it will hurt them in a delegitimatizing way.

The first Research Question (R1) was divided into three sub-questions. The first of these "What are the motivations of the perpetrators?" seems to be answered by the hackers release letter. It is in first hand to damage the organization behind the web-shop. The customers are collateral damage in this process, but they are perceived as morally guilty by the hackers, because they support the Nordic Resistance Movement economically. The next sub-question was "Do the motivations correlate with the descriptions of doxing we find in Douglas description?" and "Which of the variants of doxing is closest to their description of their motives?" also this question is possible to answer through the release letter. The motives correlates in relation to the customers. They are being exposed in a way that is similar to what Douglas describe as " delegitimatizing doxing".The customers are not the main goal for the hackers, but exposing them in a delegitimatizing way is part of their road to success in damaging the Nordfront webshop and the Nordic Resistance Movement.

COMMENT SECTION OF THE NORDFRONT "WE ARE HACKED"-ARTICLE

Nordfront release the news that their customer database has been hacked August 11, 2017. The first comment is written the same day. Later the comment section is locked due to "misuse" (Eklund 2017). All Nordfront-articles have a comment section. The comment section is regulated through moderators and a set of rules. You need to register an e-mail in order to post or link your Nordfront-comments to your Twitter- or Vkontakte-account (Nordfront: Kommentarregler 2017). Nordfront favours the russian-based social media provider Vkontakte instead of, in Sweden more popular alternatives like Facebook. This is, according to their own statements, due to the more liberal attitude towards "politically incorrect opinions" in russian social media (Nordfront: Redaktionen 2015). The comment section is divided in thread-starts and sub-threads. As a user you have the choice to comment the article directly, or answer another users comment. The "We are hacked"-article has 48 thread-starts, where a user comments directly to the thread, and in total 90 comments both thread-starts and sub-threads together (Eklund 2017). The discussion will be described below. All comment entries are connected to the Nordfront-article that has been cited before (Eklund 2017). They have been translated from Swedish to English. It is of course impossible to prove who the persons commenting are, but with a starting point in the

discourse the most likely persons to be active in this kind of comment section is a sympathizer to the Nordic Resistance Movement. Added to the translated comment is the handle, the name the person use in this online setting in brackets ("Svensk" - example). Each comment have the possibility to create a sub-thread – other internet aliases commenting on the first comment. Such sub-threads will be analyzed as a whole.

This is the main communication line to the Nordfront sphere – their own comment field. The comments are often quite short and might have been moderated by the webmasters. They claim the right to do so – even though nothing in this comment field bears evidence of any moderation. All comments that carry some substance to the discussion will be analyzed. Some are just repetition of what earlier commentators already have claimed and some comments does not. The comments have been categorized into three categories, each relating to a theme that they have been sorted into. Each category will be discussed and described below. There are 90 comments altogether with all sub-threads included, but some of these are very similar to other, so the amount that will be used is lower than this. After the comments in each category are described, a short analysis will be performed.

INFORMATION SECURITY

This category collects all comments and discussions that are about information security issues. This is, in this case, comments that are about why the leak occured. Some of these comments are short, angry, and less technically conversant. Some of them are more technically specific and tries to pinpoint what went wrong in the first place.

The first commentator after the article is posted calls himself "Svensk" ("Swedish"), the comment being angry/sarcastic "Bad Nordfront – try again – do it right". This comment starts a sub-thread where different opinions are stated. The second comments ("RSJ") states that – referring to the first comment - "Have you read the article? It is virtually impossible to protect yourself from an attack like this". This is followed by another comment ("Invisible") that states that they (Nordfront) shouldn't have saved the data for such long time, but hopefully this will have the result that more people are open with their political opinions - "We need more people that don't clench their hands in the pocket!". The last comment in the sub-thread is by "Anon"

who claims that the security on the Nordfront-page is generally low because "they use Google-affiliated services". The commentator claims to have been in contact with their IT-security officials earlier and tried to warn them. (S)he also argues that they should not have saved the customer data for such a vast period of time (from the start of the web-shop). They should have cropped the database earlier.

The second commentator, "Jostein2" (Jostein is an old male Nordic given name – still in use in Norway) states that: "There is no reason to try to protect yourself or your information on the internet. No one can protect themselves here. Even SÄPO (the Swedish Security Service) cannot protect themselves, that is why they don't connect computers with sensitive information to the Internet. Jostein2 is answered by "Anon" who comments that "even if it is hard to protect your information on the internet – you are responsible to try to do that anyway (if you are in Nordfronts position). Everything else would be defeatism."

The alias "Micke Norsk" (Mick the Norwegian) asks other users what was in the e-mail that Nordfront sent out to all those affected by the leak. He gets some short information regarding this. In the sub-thread some commentators seems to be disappointed with the e-mail. As is seems from the descriptions it was possible for each recipient to see which other mail addresses the e-mail had been sent too. This is regarded as another security breach.

Three commentators, "Joppe", "David" and "Vapensmeden" creates three different sub-threads where the amount of information saved in the customer database is discussed. Everyone who comments are very disappointed with the amount of information that has been saved over several years. Several different possible solutions are proposed. They could have warned all customers that their data will be preserved. Or they could have encrypted the customer database. "Vapensmeden" writes directly towards the person responsible for the organizations IT-security reminding them of an earlier customer database leak that occured with the publisher "Nordiska Förlagets" web-shop. Another commentator who claim to be an earlier webmaster for "Nordiska Förlaget" describes the system they used further claiming it to be much safer than the one Nordfront uses. The system described removes all customer data from servers connected to the internet withing 2-3 hours. No further discussion regarding these security suggestions are present.

"Anon" is the last commentator that will be used as an example of a statement regarding information security. This commentator is very disappointed that the web-shop did not offer secure, untraceable payment in the form of bitcoins or secure communication in the form of a TOR .onion-address. This is answered by another user ("Nordisk nationalsocialist") who claims that a shop like this must be customized towards an ordinary user, not experts in information technology. The discussion continues no further than this.

According to Dhillon et al (2004) a data-leak is to be consider to be a great obstacle for an organisation.

> Whenever an organisation experiences a computer-related crime, panic strikes and usually notmuch thought is given to the kind of controls that could be put in place. As a result, management tends to operate in a reactive mode, building on short-term gains rather than identifying longterm options or the potential negative consequences of their actions. Any occurrence of computer crime is a serious event for an organisation which could have disastrous consequences (Dhillon et al 2004, p. 1)

This must be considered valid also in this case. There are several voices in the comment field that states that this is a disaster for an organization of this sort – where participants and supporters often wants to be anonymous. The insecure e-mail sent to all customers affected by the leak could be consider to be an expression for the reactive mode that Dhillon describes.

The commentators also gives several IT-security advices. According to Paté-Cornell et al (2018) managing cyber security in an organization includes spreading the protection (which must be considered a cost) over a vast amounts of different possible risks (Paté-Cornell et al 2018, p. 1). The commentators "Vapensmeden" and "Anon" gives advice that are more technical and specific than other commentators, but most of these discussions seems to pass without the majority of the commentator noticing.

Fatalism: This category consist of comments close to the one stated by the handle "Invisible" in the first thread analyzed above – that the leak could lead to something good for the organization – that it will transform their supporters to activists that don't clench their hands in their pockets anymore. There are several comments in this category and a few of them will be discussed.

"Anders Jonsson" (a very typical Swedish name) comments in favour of the Nordfront-staff. Writing a comment mocking their enemies ("Jews and reds") and proclaiming: "You have done nothing wrong! The enemies will be crushed! Victory is the only alternative. Hail victory!". Another commentator that focus on the enemy is "Wodenwehr" who states: "Of course they (cowardly) meet you on the internet – they dare not to meet you in the streets". The commentator "Freisler" claims that: "Ok, now you know this. I have shopped for at least 2500 SEK (~$300). I am shaking with fear - Hahaha (ironical smiling face). If you read this AFA ("Anti-Fascist Action", left-wing organization and claimed enemy of the Nordic Resistance Movement) lets meet over a coffee. If you dare!". This commentator also focus on the claimed enemies and wants to proclaim that (s)he is not afraid of them. There are several examples of this attitude against the claimed enemies, another commentator, "Berserker" states that "If you, AFA, put my family or me in any danger – You are dead!"

Several other commentators claim that they don't care if their information is spread ("Waffen88", "L. B Lundholm" are two examples). Other commentators takes this another step and claim that they are more interested in the organization now, and that they will order more products from their web-shop ("Kerstin", "Hårfagersson").

The enemies of the Nordic Resistance Movement ("AFA", "Jews") portrayed in the comments are among the enemy images of the movement that Egeland-Nerheim describes in her Master thesis about this movements enemy images (Egeland-Nerheim 2015). That the enemies becomes more important to focus on when the movement is under attack is not a surprising discovery. In his book "delete – the virtue of forgetting in the Digital Age" Viktor Mayer-Schönberger claims that internet as a medium (with immense possibilities to spread information) in the long run will force persons that are the victims of doxing and other types of bad publicity to develop coping mechanisms (Mayer-Schönberger 2011, p. 154f). Focusing on the enemy, claiming that you do not care about the leak, and ordering more material could be claimed to be examples of such coping mechanisms. A way of saving yourself. Egeland-Nerheim also claims, in the work cited above, that the media strategy of Nordfront/The Nordic Resistance Movement is that "all publicity is good publicity" (Egeland-Nerheim 2015, p. 113). A leak of this sort does not need to be thoroughly bad from such a perspective.

Other: In the category "Other", comments have been placed that did not fit in the two above, more common categories. The commentators "Maximus" and "Erik", as an example, questions that an order from the shop really suggest that you are a supporter of the Nordic Resistance Movement. They claim both, that it could be ordinary persons who just found books that they thought were interesting. There is also possible, according to "Maximus" to see that some investigative journalist has bought material from the web-shop. So, what does an order really mean?

Three more commentators have not so much in common, but should be mentioned anyway because they are interesting as such. "Godnattvisa", who claims that (s)he has good knowledge in IT-security and that no web-shops, in Sweden or abroad are safe. (S)he continues and claims that informations about us is saved by everyone. That the State knows everything about us because of saved lists of library loans et cetera. "Tho" is another commentator that takes the attitude found above, when some commentators claim that they are more interested in supporting the organization now than before, a little bit further. S(he) claims that (s)he will vote for the organization in the upcoming election. And this just because of the leak, not because of any clear political affiliation. The last comment before the comment-section below the article in which Nordfront confessed ot the hacking and leak of their customer database is made by a user that call him-/herself "Vit legion" ("White legion" in Swedish). "Vit legion" writes that the leak can be changed into something good – (s)he has seen several persons in the customer database from the same small village where (s)he lives. Now the possibility exist to contact these people to start more intense political work.

Two words about delegitimization must be said in relation to the "Other"-category. First, regarding the persons mentioned above that maybe just ordered a book. Of course they also will be delegitimized by being in the database – but their presence as innocent (if known by many people) could also delegitimize the purpose of the leak. Not all people that will investigate the database will have the same strong feeling against the customers as the hackers did. Another delegitimization-related issue is mentioned by "Vit legion". The database that were supposed to be used (when leak) to delegitimize persons could suddenly be used as a contact list for political work. The persons in the database have legitimized themselves in this political discourse by ordering products from a national socialist web-shop.

CONCLUSIONS AND FURTHER RESEARCH

The first research question, regarding the motives of perpetrators (R1) where discussed exhaustive above and there will just be a short recapitulation of the answers here. The question "What are the motivations of the perpetrators?" were answered by the perpetrators in their release letter. It was in first hand to damage the organization behind the web-shop. The customers were in this case collateral damage in the process even though morally guilty (and worthy of punishment) through their support of this organization, according to the perpetrators. The next two questions: "Do the motivations correlate with the descriptions of doxing we find in Douglas description?" and "Which of the variants of doxing is closest to their description of their motives?" was also answered in the release letter. The customers were being exposed in a way that is similar to what Douglas describe as "delegitimatizing doxing". We met, and will meet, the phenomena of delegitimization further on in the conclusions.

The reactions in the comment field of the Nordfront article in which the leak became official were the subject of research question two (R2). This also has been discussed thoroughly above and the two main reactions are a disappointment with the level of implemented IT-security that the web-shop has used, and personal fatalism; commentators that claim that they don't care if they are exposed or not. It is possible to see this fatalism as a coping mechanism to deal with the leak. That such coping mechanism regarding the spread of personal information on the internet could appear have been suggested by Mayer-Schönberger as mentioned above. There is also a drift from legitimization (as customers) to delegitimization (as national socialists) to legitimization again (by being in the database - as in the comment of "Vit legion" above). We will turn back to this drift in legitimization below, in connection to the Records Continuum Model, below.

The last research question (R3) was regarding discussions of the quality of the leak. This is crucial to the purpose of the hackers (delegitimization). From their point of view we can see the customer database as a "list of names" (uncritical) of either good people (if you support the organization) or bad people (if you don't support the organization). As some commentators suggest above the reality could be more advanced that this and customers could be from a wide

range of people. Although the hackers explicitly claim that this does not matter to them it is possible that it will delegitimize their work in the eyes of other. The quality of the customer data is not discussed in any other way, which must be admitted, is a little bit frustrating from an archival point of view.

Finally, what kind of further research could be done? One possibility would be to discuss leaks of this kind using a larger amount of archival theory. There are openings to connect theories of legitimization/delegitimization to the Records Continuum Model where a leak could be a part of the "pluralize"-phase of the model (Upward & McKemmish 2006, p. 225). The possibility that records and archival matter leak and then is used to delegitimize a person would be interesting to investigate using different cases. The stretch from legitimization/delegitimization and then legitimization again that could be observed in the investigated material above could be tried against other leaks in other context to confirm or deny if it is a process that generally occur during leaks of politically sensitive material connected to persons. But this would be an investigation to be undertaken in the future.

References

Andreasson, Jesper & Johansson, Thomas (2016) "Online Doping. The new self-help culture of ethnopharmacology" *Sport in Society* 19:7, p. 957-972.

Dhillon, Gurpreeet, Silva, Leiser, Backhouse, James (2004) "Computer Crime at *CEFORMA*: a case study. *International Journal of Information Management* 24:551-561.

Douglas, David M (2016). "Doxing: a conceptual analysis" *Ethics and Information Technology*, 18:199-210.

Egeland-Nerheim, Elise (2015) "Nordfront og nettekstremisme - Den nordiske motstandsbevegelsens fiendebilder". Master thesis, Agder University.

E-Handel (2017) "Politiker handlade i nazistisk webbshop – avgår" retrieved 2018-10-19 from http://www.ehandel.se/Politiker-handlade-i-nazistisk-webbshop-avgar,10910.html

Eklund, Robert (2017) "VIKTIGT MEDDELANDE: En av Nordfronts servrar har hackats" Nordfront.se , August 11, 2017, retrieved (and printed) 2017-08-29 from https://www.nordfront.se/nordfront-har-hackats.smr

ETC (2017) "Här är SD-politikerna som stöttat nazistgruppen" retrieved 2018-10-19 from https://www.etc.se/inrikes/har-ar-sd-politikerna-som-stottat-nazistgruppen-nmr

ETC (2017) "SD-topp medlem i nazistgrupp" retrieved 2018-10-19 from https://www.etc.se/inrikes/sd-topp-medlem-i-nazistgrupp-en-god-sak

ETC (2017) "Marduk revealed with ties to neo-nazi party" retrieved 2018-10-19 from https://www.etc.se/kultur-noje/marduk-revealed-ties-neo-nazi-party

Expo (2018) "Nordiska Motståndsrörelsen" retrieved 2018-10-01 from https://expo.se/fakta/wiki/nordiska-motstands%C2%ADrorelsen

Expressen (2017) "KD-politikern avgår – Köpte nazistpropaganda" retrieved 2018-10-01 from https://www.expressen.se/gt/kd-politikern-avgar-kopte-nazistpropaganda/

Flashback (2017) "Nordfront förlags kundregister på vift", retrieved 2018-10-19 from https://www.flashback.org/t2863374

Malmqvist, Karl (2015) "Satire, racist humour and the power of (un)laughter: On the restrained nature of Swedish online racist discourse targeting EU-migrants begging for money", *Discourse & Society*, vol 26(6), p. 733-753.

Mayer-Schönberger, Viktor (2011) *delete – The virtue of forgetting in the Digital Age*. Princeton: Princeton University Press.

McLuhan, Marshall (2005) *Understanding Media – The extensions of man*, London: Routledge.

Månsson, Josefin (2014) "A dawning demand for a new cannabis policy: A study of Swedish online drug discussions" *International Journal of Drug Policy*, no. 25, p. 673-681.

No Front Friday (release letter) last modified 2017-08-11 https://nopaste.me/view/raw/aac5e89a

No Front Friday (customer database) last modified 2017-08-11 https://nopaste.me/view/raw/1e63d7ff

No Front Friday (twitter account), accessed 2017-09-02 https://twitter.com/nofrontfriday

Nordfront: Kommentarregler (2017), accessed 2018-10-29 https://www.nordfront.se/kommentarregler

Nordfront: Redaktionen (2015) "Nordfront har nått 500 följare på VK.com", October 21, 2015, Accessed August 29, 2017, https://www.nordfront.se/nordfront-har-natt-500-foljare-pa-vk-com.smr

Nordic Resistance Movement (2017) *Our path.*

Paté-Cornell, M.-Elisabeth, Kuypers, Marshall, Smith, Matthew, Philipp, Keller (2018) "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies" *Risk Analysis* vol 38, no 2.

Pickard, Alison Jane (2013) *Research Methods in Information.* London: Facet Publishing.

Swedish Election Authority (2018) "Election result", retrieved 2018-10-01 https://www.val.se/servicelankar/other-languages/english-engelska/election-results-2018.html

Thomassen, Theo (2001) "A first introduction to Archival Science" *Archival Science* 1: 373-385

Traditional Youth Network "Nordic Resistance Movement Manifesto: Now in English" retrieved 2017-08-25 from (now defunct) http://www.tradyouth.org/2016/12/nordic-resistance-movement-manifesto/

Upward, Frank & McCemmish, Sue (2006) "Teaching record keeping and archiving in continuum style" *Archival Science* 6:219-230

Urban Dictionary: 1337, last modified 2003-04-24 http://www.urbandictionary.com/define.php?term=1337

VICE (2017) "Doxxing White Supremacists is making them terrified" retrieved 2018-10-19 from https://broadly.vice.com/en_us/article/7xxbez/doxxing-white-supremacists-is-making-them-terrified

Westerlund, Michael, Hadlaczky, Gergö, Wasserman, Danuta (2015) "Case study of posts before and after a suicide on a Swedish internet forum" *The British Journal of Psychiatry*, 207, p. 476-4