

# Indicators of Information Warfare

Torkjel Søndrol, Anders Wiehe, Roar Sollie, Morten Sporild,  
Ole Martin Dahl, Fredrik Skarderud and Ole Kasper Olsen

6th October 2004

## Abstract

In this report we discuss information warfare in crisis and everyday life. We also locate indicators of such attacks in some chosen cases. The report will cover three different cases where information warfare is conducted; war and terror, product marketing and internet banking.

## Contents

<b>1</b>	<b>Information Warfare in War and Terror Situations</b>	<b>2</b>
1.1	Terror Situations . . . . .	2
1.2	Information Warfare During the Chechen War . . . . .	3
1.3	Indicators on Information Warfare . . . . .	3
1.4	Summary . . . . .	4
<b>2</b>	<b>Information Warfare and FUD</b>	<b>5</b>
2.1	Indicators on Information Warfare . . . . .	5
2.2	Microsoft's FUD Campaigns . . . . .	6
2.3	Summary . . . . .	7
<b>3</b>	<b>Information Warfare and Online Banking</b>	<b>7</b>
3.1	Indicators on Information Warfare . . . . .	8
3.2	Summary . . . . .	11
<b>4</b>	<b>Conclusion</b>	<b>11</b>

# **1 Information Warfare in War and Terror Situations**

Though only a small part of information warfare is committed during wartime, we will start this article describing the use of information warfare in war and terror situations.

## **1.1 Terror Situations**

Michael Vatis[1] describes some examples of information warfare from a terrorists point of view in his article. One example was the 1997 Tamil Tiger hacker attack on Sheffield University, England, where they used the university network to spread propaganda and get extra funds. They managed to perform this covertly, and obtained user IDs and passwords from legitimate users and respected academics at the university. They used their accounts to spread e-mails all over the world asking for money to a charity in Sri Lanka. In addition, they launched a DoS attack against the Sri Lankan government center.

Another example is one where computers were used for storing information used in terrorist actions. When the police arrested Ramzi Yousef, the mastermind behind the World Trade Center bombing, they found the whole plot for blowing up 11 American airlines in the pacific on his laptop. The files was encrypted, but the FBI was able to decrypt the data, since the program used to encrypt also was on the laptop (with the encryption key).

The Defence Information Systems Agency detected 250,000 attacks against the American Department of Defence's systems in 1995. It is difficult to know whether an hacker attack is a cyber-terrorist attack or performed by a bored teenager. For instance, in 1996, a series of attacks was made against the telecommunication systems in the southeastern part of the US. The attacks was focused on the 911 emergency system in Florida. It turned out that the attack was performed by a hacker in Sweden, but it was unclear whether his purpose was to deny access to legitimate user or test his own skills.

## **1.2 Information Warfare During the Chechen War**

Information warfare has been used in wartime as long as there has been wars. Like Sun Tzu said: *Conquest your enemy without warfighting is the best way to win*[2]. This might be the first aim at information warfare. According to Dr. Graeme P. Herd[3], there were many examples of information warfare during the Chechen wars. The first Chechen war was a disaster for Russia. They did neither gain nor hold information advantage over the Chechen fighters and the public opinions forced Moscow to abandon its military campaign, particularly the electronic media. Large television channels, such as NTV <sup>1</sup> showed live footage of dead, maimed and captured Russian soldiers. At the beginning of the second Chechen war, the Russians understood there were two wars to be fought; the actual military war and the information war. They used self-censorship to shape the military response, and criticized foreign news reporters, like *Reuters* and *The Associated Press* for being working for the foreign intelligence services. During the battle of Grozny, the Russian media reported that the Russian military units used Chechen elders and published their own local news sheets to build bridges with the local community. But the Russians also lost a lot of information battles, like the threats of EU sanctions and the withdrawal of Council of Europe status. There were also reports in the west on how the Russians used chemicals, biological weapons, fuel air explosions and concentration camps, which the Russians later disclaimed as rebel propaganda. There were several disagreements regarding the body counts during the wars. The *Kavkaz Tsentri* web site stated that civil casualties exceeded 10,000 people, which the Russian Colonel-General claimed should be 'divided several times over'. This example shows how information warfare was used during war to manipulate the media from both Russian and Chechen side.

## **1.3 Indicators on Information Warfare**

### **1.3.1 Indicator 1 – Spreading Propaganda**

Terror organizations use information warfare to spread fear among normal citizens in order to proclaim their visions. As seen in the Tamil Tigers case and the

---

<sup>1</sup>NTV Russian national TV

World Trade Center case (1.1), a hacker attack spreading propaganda might be an indicator of information warfare. But without knowing the source of the attack and the reason, it is impossible to know (something the Swedish hacker attack is an example of, see 1.1).

### **1.3.2 Indicator 2 – Group Identification**

If we know the source of the attack and the motivation, we can say that attacks from well-known terrorist organizations can be indicators of information warfare.

### **1.3.3 Indicator 3 – Attack on Infrastructure**

Former president Clinton defined in 1996 the following critical national infrastructure: electric energy, gas and oil storage and transportation, telecommunication, bank and finance, transportation, water supply, emergency services and continuity of government services. Using Clinton's definitions, we can say that any attack on the infrastructures could be indicators of information warfare. Also any attempts on mapping any of the infrastructures might be preparation for an information warfare attack, but again, like the Swedish example in 1.1 there is no way of knowing whether it was only a bored teenager without knowing the source and motivation.

### **1.3.4 Indicator 4 – The Use of Media**

Dr. P. Herd said [3] that to win a war it has been almost axiomatic you have to gain public support at the outset of military operations, present the defence missions positively to maximize support and present policy both at the outset and during war. 1.2 shows many examples on how the media was used to gain public support during the Chechen War. The use of media during wartime is therefore an indicator of information warfare.

## **1.4 Summary**

Information warfare during war and crisis has been around for centuries, however with today's information and communication technology conducting information

warfare attacks are becoming much faster, easier and more widespread.

## **2 Information Warfare and FUD**

Fear, Uncertainty, and Doubt or FUD is a information warfare tool originally perfected by IBM [4][5]. If you can spread disinformation about your competitors' products, you may be able to get them to buy your product instead. FUD's primary goal is to scare customers from using other companies' products. FUD is often easy to disguise. Spotting such a campaign is therefore difficult, especially when hidden between other facts or half-truths.

### **2.1 Indicators on Information Warfare**

There are several indicators that can be used in a FUD information warfare campaign[4]:

#### **2.1.1 Indicator 1 – Urgency**

This indicator relies on time as a factor of when you should acquire the product. It uses statements like "You must buy this product today!" often to avoid a problem tomorrow.

#### **2.1.2 Indicator 2 – Supporters**

Find a trustworthy source to recommend your product e.g. Norwegian dentists who are recommending Extra sugar free chewing gum. This doesn't necessary mean you should purchase this product, but chewing gum in between meals are good in general.

#### **2.1.3 Indicator 3 – Technical**

Commercials are known to use large and fancy words for endorsing their product. Using scrumptious instead of well known words as delicious makes your product sound better. One can also use hyping of a specific technique, e.g. if you're

selling broadband and your commercial says: "this product uses TCP/IP!", non-technicians might be impressed with this, even though it's the standard on Internet. This approach is also referred to as buzzword compliance.

#### **2.1.4 Indicator 4 – Harm**

You will be worse off without this product. E.g. "if you don't buy this IDS, you will be hacked, your business will loose market share or without it you will loose time and money".

#### **2.1.5 Indicator 5 – Spin Doctoring**

Focusing on your opponent's weaknesses instead of comparing strengths. Convince the buyer of not purchasing their product, so that they will buy yours instead. Much like discussed in the next section with Microsoft's FUD strategy against GNU/Linux.

## **2.2 Microsoft's FUD Campaigns**

There have been many rumours about a lot of FUD campaigns in the media and on the Internet, and after about 1990 this weapon has been more and more frequently associated with Microsoft.

An example is FUD campaigns that Microsoft launches against the open source community. A whitepaper written by Microsoft [6] explains the hospitality of GNU/Linux in the retail market. This paper spreads a lot of disinformation or at least states facts about GNU/Linux that never have been proven truthful, e.g. that GNU/Linux is less secure than Microsoft Windows. Saying that Microsoft Windows is more secure than GNU/Linux or the opposite is almost impossible to answer, it all depends on how you measure the operating system (OS), which criterions you look for and what the OS is set up to do[7]. The paper also uses heavy propaganda for selling Microsoft products, this is of course acceptable, but could be considered a part of an information warfare attack against GNU/Linux. The white paper also promotes Commercial Off-The-Shelf Software (COTS) as being better than open source software. The debate of COTS versus open source

software is discussed by several security experts around the world. A common answer to which solution is the most secure is that there is no correct answer[8] just like the answer on which is the most secure MS Windows or a GNU/Linux OS distribution.

Microsoft also released a "competitive guide" on Microsoft Office vs. OpenOffice [9]. This document contains a comparison between the two office suites. Taran Rampersad has broken down this document [10] and found several misleadings and direct errors.

### **2.3 Summary**

To summarize this section we can say that FUD or spreading Fear Uncertainty and Doubt could indeed be an indication and a part of an information warfare attack.

## **3 Information Warfare and Online Banking**

The following is a real case, where claims about poor security were aimed at Skandiabanken, a pan-Scandinavian online banking service, and published in Norway's leading economical newspaper, Dagens Næringsliv [11].

As the largest bank in Norway which only has a presence online, Skandiabanken is a lucrative bank to break into, or perhaps even better—publish vulnerabilities about.

In a report entitled "How Secure are Norwegian Online Banks" [12] credited to three professors and two Ph.D. students at the University of Bergen, claims are being set forward that Skandiabanken's security is extremely poor. It is to be noted that although the title may indicate otherwise, no other banks have been subject to analysis.

The report is based on a master thesis [13] which contains a section which in a balanced way describes some weaknesses in Skandiabanken's security system as of 2003. In short, the thesis uncovered that given some demographic insight, an attacker will be able to generate valid Skandiabanken login credentials (social security numbers). Given that Skandiabanken only uses passwords with length of

4 digits, it is highly probable that an attacker would be able to gain access to some (maybe as many as 10 to 20) random accounts.

This is the entirety of the Skandiabanken vulnerability. An attacker may be able to gain access to a few random accounts using brute force methods. Obviously this would be a pretty difficult attack to mount, as Skandiabanken probably has intrusion detection systems going, and many accesses from the same computer in a short period of time would probably be detected. It is *extremely* improbable that an online banking service does not log unsuccessful login attempts. To prevent detection, the attacker might spread the attempts over a large time span or use some sort of distributed network ala distributed denial of service zombies. Unfortunately, Skandiabanken stores an account's creditcard number and expiration date in plain view for anyone with access to the account, hence using a considerable amount of time to attack Skandiabanken might actually pay off. If credit card information was not available on the account pages, the break-in would probably only reveal some information about the random victim's consumer pattern, as moving money around without leaving an electronic trail is difficult.

However, this was the situation in 2003. Skandiabanken's security system is now upgraded with another layer of security which requires that you receive a onetime password either on a mobile phone or via mail to be able to download the certificate which authenticates you towards the server. If received on mobile phone the password times out after 15 minutes, 14 days if received by mail.

### **3.1 Indicators on Information Warfare**

#### **3.1.1 Indicator 1 – Instills Fear in the Reader**

The article does what it can to instill fear in the reader and to make the findings more sensational than they really are.

For example, when using phrases like the following, which is freely translated from Norwegian, they knowingly exaggerate their own findings to make it have more impact on the reader.

*”Unfortunately we found that it was possible to determine both social security numbers and PIN codes for persons who already were*

*customers of the online bank”*

All they are able to determine are the social security number and PIN<sup>2</sup> code for a couple of *random* customers, hence this is an exaggeration of their findings to instill fear in readers who are also customers of Skandiabanken.

### **3.1.2 Indicator 2 – Unnecessary and Sensationalistic Content**

The report makes a large point out of the fact that they managed to register a non-existent person by using the social security number of a dead person and the name "Bill Gates" into the systems of Skandiabanken. However, with regards to the security of the online bank solution, this is completely unnecessary information which doesn't really have any value whatsoever. It is not evidence of poor security, nor is it evidence of lax implementation or routines as the report claims.

Should Skandiabanken gain realtime access to the Norwegian personal register to see if a social security number belongs to a dead person when the attempt to register is being made? Hardly necessary when the password for gaining access to the online banking system is sent by registered mail to the person who match the social security number. Should Skandiabanken start screening for special names? Obviously not.

This entire case is totally blown out of proportions to be made into sensational news.

### **3.1.3 Indicator 3 – Lies and Half Truths**

The report also claims that Skandiabanken's PKI solution is bad, and they more than insinuate that Skandiabanken or the ones who developed their online banking service did not fully understand the basics of PKI, hereunder use of client and server certificates along with SSL/TLS.

A description of the TLS protocol and related technologies is out of the scope of this report, but given some insight into these technologies, it is easily understood that Skandiabanken's PKI implementation is adequate. Skanidabanken authenticates itself to the client with a certificate issued from an acknowledged Certificate Authority. Skandiabanken then has its own Certificate Authority which

---

<sup>2</sup>Personal Identification Number

issues certificates to users which again authenticates the client to the server. The weakest link here is the issuing of the client certificate, as the authentication here is based on a less secure authentication mechanism, namely the social security number and PIN code combination which [13] has proven to be too weak.

As previously mentioned, Skandiabanken has now added a new layer of security in which a one time password is sent to the rightful owner's mobile phone by SMS. The report claims that it is elementary to tap communication to and from a mobile phone, and that equipment for doing so can be easily obtained<sup>3</sup>. Yes, it is perhaps possible, but can this be made into a practical attack? We think not.

Given the three pieces of information a user needs to know to be able to gain access to a Skandiabanken account (social security number, PIN code and one time password obtained from the user's own mobile phone), the authentication is good.

#### **3.1.4 Indicator 4 – Buzzwords Out of Context**

Although not mentioned in [12] itself, when presenting their case to the media, the authors are cited on saying that Skandiabanken's online banking service is based on "security by obscurity", which is a common term within the information security community which refers to security which is implemented in such a way that public disclosure of the underlying algorithms would totally break the security.

Skandiabanken's security is not "security by obscurity". Skandiabanken makes use of common, well-known and well-understood protocols and encryption algorithms. Nothing about what is revealed in [12] has anything to do with "security by obscurity", and it seems that Hole uses the phrase as means to impress the public with fancy words they don't understand. For more about "security by obscurity" we refer to [14].

---

<sup>3</sup>The authors of [12] are themselves referring to such a device in a talk given on the subject. The device which supports SMS extraction costs \$420,000 in purchase and will crack the GSM encryption in 15 minutes (by which time the password will no longer be valid).

## **3.2 Summary**

The report is a sensationalistic spin on some balanced findings in a master's thesis. While anyone would acknowledge that SkandiaBanken really should expand their PIN codes to more than only 4 digits—perhaps use fullfledged passwords of at least 8-10 letters in length—the findings are presented in the report in an overly dramatic and exaggerated fashion to make some sensational headlines.

If the paper had been picked up by the major Norwegian newspapers, it could very well have had a negative effect on Skandiabanken. In this case, excepting Dagens Næringsliv [11], only a few semi-serious Norwegian online newspapers picked up the original story with the same spin as [12].

It is to be noted that even though an expansion of the PIN codes is clearly recommendable, such a major operation might not be beneficial to Skandiabanken as the cost of providing every customer with a new password and help during the transitional phase would be high. Also, as Odlyzko argues in [15], for something to be secure yet economically viable, providing enough speed bumps are usually enough as that will sufficiently deter an attacker.

## **4 Conclusion**

To conclude the examples we have examined, we can see that information warfare or at least indicators on information warfare is very much alive in a great part of today's society whether in war or business competition. It can be hard to discover if a campaign is part of an information warfare attack or just an error, misinformation, vandalism etc. Everyone should be critical to things they read and hear.

## References

- [1] Michael Vatis. *Cyber Terrorism and Information Warfare: Government Perspectives*. <http://www.terrorismcentral.com/Library/Teasers/vatis.html>, 2001.
- [2] Sun Tzu. *The Art of War*. Running Press Book Publishers, miniatures edition, July 2003.
- [3] Graeme P. Herd. *Information Warfare & the Second Chechen Campaign*. <http://www.da.mod.uk/CSRC/documents/CEE/G81/G81.chap6>, 2003.
- [4] Brian Martin. *The Newbie's Guide to Fear, Uncertainty, and Doubt*. <http://www.attrition.org/~jericho/works/security/fud.html>, 1999.
- [5] Eric Green. *FUD101*. <http://badtux.org/home/eric/editorial/fud101.php>, 1999.
- [6] Microsoft Cooperation. *Linux in Retail & Hospitality What Every Retailer Should Know*. <http://whitepapers.zdnet.co.uk/03902594560075980p39000684q00.htm>, 2001.
- [7] Illena Armstrong. *Windows vs. Linux: Taking Security Seriously*. <http://www.securityfocus.com/library/3446>, 2001.
- [8] Andy Jones, Gerald L. Kovacich, and Perry G. Luzwick. *Global Information Warfare*. Auerbach Publications, 2002.
- [9] Microsoft Cooperation. *OpenOffice 1.1 Competitive Guide SMB Segment*. <http://members.microsoft.com/partner/salesmarketing/opensource/discguides/OpenOffice.pdf>, 2002.
- [10] Taran Rampersad. *Microsoft displays fear, uncertainty, and doubt toward OpenOffice.org*. <http://software.newsforge.com/software/04/03/27/0134204.shtml>, March 2004. Comments on [9].

- [11] Dagens Næringsliv. *Slakter nettbank-sikkerhet*. Newspaper, pages 72-73, 4th September 2004.
- [12] Kjell Jørgen Hole, Øyvind Ytrehus, Tor Hellesteth, Thomas Tjøstheim, and Vedbjørn Moen. *Hvor sikre er norske nettbanker?* <http://www.nowires.org/nettbanker/nettbanker.pdf>, September 2004.
- [13] Thomas Tjøstheim. A critical view on public key infrastructures. Master's thesis, University of Bergen, 2004.
- [14] John Viega and Gary McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley Pub Co, 1st edition, September 2001.
- [15] A. M. Odlyzko. Economics, psychology, and sociology of security. In R. N. Wright, editor, *Lecture Notes in Computer Science vol. 2742*, pages 182–189. Springer, 2003.