Mobile Security from an Information Warfare Perspective

Brett van Niekerk and Manoj Maharaj
School of Information Systems and Technology
University of KwaZulu-Natal
Westville, South Africa
991160530@ukzn.ac.za

Abstract— **With the increasing prevalence of mobile devices, there is an increasing risk that the mobile networks may be targeted by information warfare attacks. An investigation of mobile security issues from an information warfare perspective, with emphasis on computer network warfare and electronic warfare, is presented. The paper focuses on analysing prior cases of mobile security breaches from an information warfare perspective, however previous research is also discussed. The validity of the various potential and perceived threats to mobile security is discussed. Preliminary results from current research into mobile security and information warfare are reported; initial simulation results assessing the practicality of jamming and eavesdropping on 3G signals and the responses from first round of research interviews are discussed.**

Keywords- mobile security, information security, information warfare, vulnerability analysis

I. INTRODUCTION

Recently there have been two major security incidents affecting the mobile phone industry; the Vodacom SMS Banking [1] fraud and the release of a how-to guide on cracking the A5/1 stream cipher used [2, 3] for the Global System for Mobile Communications (GSM) networks. This naturally calls into question the security of mobile phones; which is of concern especially due to the increasing prominence of mobile phones in society and their use in e-commerce and e-government related services. The possibility of information warfare utilising mobile infrastructures and devices is highlighted in [4].

The paper discusses the security of mobile phones from an information warfare perspective. Information warfare is the concept of information being used as a weapon as well as being a target [5]; it aims to corrupt, deny, degrade and exploit information and information systems and processes [6], thereby affecting the confidentiality, integrity and availability of the information and their supporting systems. Information warfare is comprised of a number of disciplines; of particular relevance to mobile phones is electronic warfare and computer network warfare.

Section II provides the background to information warfare and the mobile telephone infrastructure. Section III will discuss previous research and prior security incidents involving the mobile infrastructure. Section IV presents results of the authors' current research into mobile security and information warfare.

II. BACKGROUND THEORY

Here the background theory to the mobile phone infrastructure and information warfare is presented.

A. Mobile Phone Infrastructure

This section provides an overview of the operation of the cellular telephone networks and their interconnections with the public switched telephone network (PSTN) and the Internet.

The reason for the term 'cellular phone' is that the signal coverage is divided into cells, and all users in that cell connect to that base station, or cell phone tower. They are free to roam in the cell, or between cells, where they will be 'handed over' to the relevant base station. The link from the base station to the mobile stations is known as the downlink, and the connection from the mobile station to the base station is the uplink [7]. In South Africa uplink and downlink use the GSM standard, with Wideband Code Division Multiple Access (WCDMA) being the primary Third Generation (3G) standard employed for the wireless links. Another 3G standard that is commonly used is Code Division Multiple Access 2000 (CDMA2000) [8].

The base stations connect together into a network using wireless microwave links or fibre-optic cable via a mobile switching centre (MSC) [9]. This network also connects to the PSTN from the MSCs, enabling calls to connect between the cellular networks and the fixed-line infrastructure. The network is also connected to other external entities, such as the internet, where one may send SMSes (Short Messaging Service) to cell phones. These are known as External Short Messaging Entities (ESME). This then connects to the Short Messaging Service Centre (SMSC) that routes all SMS traffic [9].

B. Information Warfare

The concept of Information Warfare first gained prominence in the early 1990's [6]; yet a number of the constituent methods and tactics are much older. Two principles of information warfare are that information has value [10], and

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

information and information systems can be considered both as weapons and targets [5]. The aim of information warfare is to corrupt, deny, degrade and exploit adversary information and information systems and processes [6], and protect the confidentiality, integrity and availability of one's own information and the relevant systems. Information warfare tactics may attempt to impact on the military, political, economic and social domains [5]. The South African National Defence Force identifies six functional areas of information warfare (shown in Fig. 1), namely [11, 12]:

- **Command and Control Warfare:** protecting one's capability to effectively command, control, and manage one's forces while attempting to disrupt an adversary's command and control capacity [11].
- **Intelligence Based Warfare:** maximising one's intelligence gathering and processing capabilities whilst degrading those of an adversary [11].
- **Information Infrastructure Warfare:** protecting one's own information infrastructure (which includes other infrastructure upon which it is dependent) whilst attacking or exploiting an adversary's [11].
- **Electronic Warfare:** preventing an adversary's use of the electromagnetic (EM) spectrum whilst preserving its availability for one's own use [11].
- **Network Warfare:** protects one's information networks whilst attack or exploiting an adversary's information networks [11].
- **Psychological Operations:** planned, and coordinated activities undertaken to influence the emotions, reasoning and behaviour of a target audience in order to further one's objectives [11].

These areas may be grouped into two domains: the application domain, comprising of command and control warfare, intelligence based warfare and information infrastructure warfare; and the enabling domain, comprising of electronic warfare, network warfare and psychological operations [11, 12]. The enabling domain creates affects in the application domain [11, 12].

Relating the information warfare functional areas to the mobile phone infrastructure; electronic warfare will target all the wireless links, and network warfare will target any internet or network connections or services. Information infrastructure warfare will encompass the entire mobile infrastructure. The infrastructure may be used for command and control, or distributing psychological operations messages. Should the mobile phone infrastructure become compromised, it may be possible to exploit it for intelligence based warfare.

III. Incidents and Previous Research

This section will discuss previous research and assess the impact of this research on the security of the mobile infrastructure. A number of cases where a mobile infrastructure has been compromised or exploited will also be described. For each case, the relevance of the incident to information warfare and future mobile infrastructure security will be discussed.

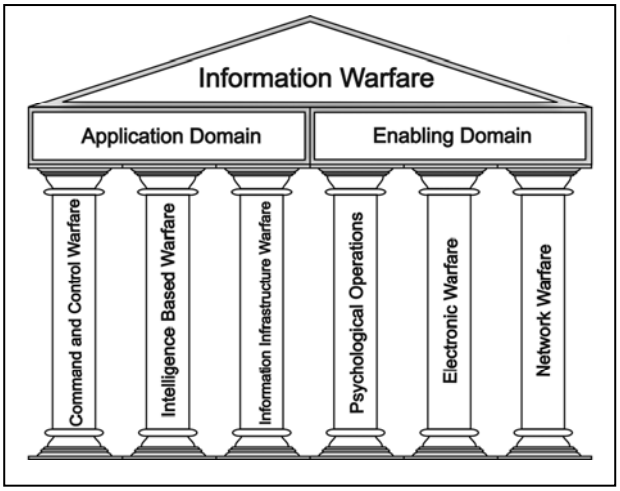

Figure 1. Information warfare functional areas

A. Disgruntled Employee

In 1999 a disgruntled employee hacked into the Vodafone messaging network and sent SMSs to over 30,000 international subscribers stating that they had won a car, and should phone the his previous employer to claim the prize [13, 14]. This illustrates that there is a valid threat to mobile phone networks from all areas of society; someone with knowledge of a system could gain access to the infrastructure for nefarious purposes. The result of this incident was an influx of calls which blocked the switchboard and brought the firm's business to a halt and cost an estimated £10,000 [13, 14]. This attack was motivated by revenge; however a group wishing to cause more damage could use network warfare tactics to conduct information infrastructure warfare with a more serious impact.

B. Greek Cell Phone Espionage

This incident, also known as the Athens Affair, saw the mobile communications of over 100 high-ranking dignitaries, including the Greek prime minister, compromised due to sophisticated eavesdropping through the manipulation of Vodafone Greece's network components [15]. It is still unclear whether the attackers penetrated the system from the outside or had insider assistance, and it is unknown if recordings were made of any compromised phone calls [15]. The system was compromised just prior to the August 2004 Olympic Games, and was detected in January 2005 [15]. Rogue software was found on four of the MSCs, which subverted the legitimate built-in wiretapping features of the network [15]. The software created parallel streams of the digital voice of the phone call; the original stream between the two users remained, and a copy of the call was sent to other cell phones (along with location information which was sent via SMS) which enabled the attackers to listen in on or record the conversations [15].

The advantage of compromising the switches is that it is the core of the network, therefore the major switches carry the majority of the traffic; and the data through the switches is not encrypted, whereas the GSM wireless links are [15]. Nevertheless, the manipulation of the switch was complicated; intruders had to install and operate the wiretapping software, and occasionally access it to alter the target phone numbers or

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

eavesdropping receivers, all without the system administrators knowing, without creating logs or the additional code being discovered; reference [15] explains how this was done.

This incident illustrates the use of network warfare to compromise a mobile phone network in order to conduct intelligence based warfare. It also shows that providing a legitimate means for wiretapping may aid potential intruders, as it was specifically the wiretapping function that was targeted; this has implications for the Regulation for the Interception of Communication Act in South Africa. For this act to be effective similar legitimate wiretapping functions need to be present, providing the opportunity for the switching centres to be compromised as in the example above, or the possibility of individuals impersonating law enforcement officials gaining access to the wiretapping function.

C. The SMS Banking Scandal

In July 2009 a Vodacom engineer and a co-accused were arrested in South Africa for creating duplicate SIM cards in order to intercept the one-time passwords that banks sent to their client via SMS for internet banking [1]. It is estimated that their efforts managed to steal over R7 million from banking clients [1]. Information that was used to identify targets and aid the password interception was gathered through phishing attacks [16]. It appears that some form of social engineering (psychological operation) was employed to coerce the Vodacom engineer in co-operating with the external gang [1]. Through the engineer, the gang was able to compromise the confidentiality of both the mobile phone network and the financial institutions. This illustrates the relevance of the insider threat to mobile security. This also may open the possibility of using an attack similar to the Greek espionage incident described above to intercept the passwords.

D. The GSM Project

The GSM Project is attempting to break the A5/1 stream cipher used in GSM mobile phone communications to protect the wireless link [3]. The effort is using distributed computing to generate a large look-up table which could be used to crack encryption on GSM networks [3, 17]. The GSM Alliance believes that the codebook will be large; approximately 2TB, and that the process will still be complex and special equipment will be required to intercept the mobile phone signal [17]. The eavesdropper also needs to be close enough to the cell phone to intercept the signal. Therefore, to do mass interceptions such as the Greek incident, this method is not practical. Due to the complexities this capability beyond most individuals, whereas other groups and governments have access to more sophisticated and effective methods. The project was not intended to actually be used, but to create awareness of possible vulnerabilities and coerce the mobile phone operators to improve the security of their networks [3].

E. Mobile Phone Viruses

The Cabir mobile phone virus first detected in June 2004, and was limited to the Symbian-60 operating systems and Bluetooth capable phones [18]. The Skulls virus also targets the Symbian series operating systems and is distributed via Bluetooth; it disables all system applications, therefore usually only the phone functionality remains [19]. These viruses prove the concept of using mobile phones as a platform for distributing viruses, and also the transmission of viruses over Bluetooth services. The CommWarrior virus also had the capability of propagating via the multimedia messaging service (MMS), however user interaction was required [20], indicating a degree of social engineering. The propagation of mobile phone malware was modelled in [21], which shows that the propagation by MMS may result in severe degradation of the MMS service due the central MMS server becoming congested.

In March 2010 it was found that Vodafone HTC Magic smartphones in the UK that were running Google's Android software contained a Mariposa bot client that sent the users' passwords and credentials when it was connected to a PC [22]. There is also a range of spyware, worms and exploits that target the iPhone, most of which compromise the phone's content [23]. This again shows the concept of using mobile phones to distribute malware, in this case to 'gather intelligence' on users' confidential information. India has recently banned the importation of Chinese manufactured cell phones and infrastructure components due to a fear of malware that could compromise the privacy of India's mobile networks [24].

From an information warfare perspective, these examples illustrate the possibility of using viruses and malware as offensive network warfare not only targeting computer networks, but also the mobile phones networks. This could increase the effectiveness of an information warfare attack, and also increase the psychological impact of that attack.

F. Other Incidents

The mobile phone networks may be used as a tool for mass distribution of propaganda, psychological operations messages and hate speech, as occurred in Kenya after the December 2007 elections, further inciting the violence between the ethnic tribes [25]. There are also reports of Israel hacking into Lebanese telephone and mobile phone networks and spamming users with SMS and voice mail messages offering rewards for information on missing Israeli soldiers and distributing anti-Hezbollah messages [26].

These incidents illustrate the use of the mobile phones for psychological operations. Once the mobile network has been compromised via network warfare, mass messages may be sent in order to influence a population's perceptions. Legitimate SMS tools may also be utilised for this purpose.

Phishing scams have also begun to appear on mobile phones in South Africa [27]; the migration of scams to mobile phones was predicted in the United States in 2005 [9, 28]. There have also been a number of incidents where users have been billed for, and even had money debited from their bank accounts, due to problems with SMS subscription services [29]. Similar problems could be exploited by groups as business intelligence, or to illegally fund operations through this fraud. The increase in the use of mobile phones for social networking applications and email may further expose users to these attacks.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

In June 2010 it was found that the iPad 3G services were breached; over 100 000 high ranking persons in the United States had their emails and associated SIM card authentication compromised [30]. This again illustrates the vulnerability of 'smart' mobile devices.

G. Exploitation of SMS Services

Reference [9] illustrates the possibility of saturating a localised area with SMSs; should sufficient SMSs be distributed, even voice calls in the affected area could be denied. The principle is that a compromised web-based ESME could be used to flood mobile networks with spam SMSs, overwhelming any bottlenecks in the mobile network [9]. The possibility of targeted attacks is also mentioned, where a few individuals could have their mobile phones flooded with spam in order to prevent legitimate messages and voice from reaching the devices [9].

This research again illustrates the susceptibility of mobile networks to a network warfare attack via the internet. The advantage to this type of an attack is that it can originate from anywhere in the world, and potentially affect larger areas; traditional jamming requires the jammer to be within a certain range of the target. With the introduction of high bandwidth technologies, a general attack may not be as successful due to the required amount of spam SMSs; however it is still a possibility. From a South African perspective, the mobile networks are grouped according to the network service provider, and not according to regional area as in the U.S. where the investigation took place [9]. South African mobile networks may be more resilient to such an attack as it may need to overwhelm a nation-wide network in order to be successful.

It is also possible to use an SMS injection attack which crashes the connectivity on a number of smart phones; this prevents the user from connecting to GSM, 3G or WiFi networks [31]. This is effectively a denial of service attack against the mobile device itself.

H. Summary

The majority of incidents illustrate the use of network warfare to compromise the security of mobile networks in order to accomplish various objectives; the insider threat is also realised. Standard information security practices should be sufficient to prevent such incidents from occurring; firewalls and intrusion detection systems may be employed to mitigate the threats by controlling the linkages on the mobile phone infrastructure to the internet. However, information security policies and hardware and software configurations need to be effective and kept up to date, just as in computer networks. Conducting awareness campaigns for the public and employees may mitigate the insider threat, the success of phishing attacks, and malware propagation. With the increasing prevalence of smartphones with mobile computing and connectivity capabilities, the overlap between the mobile network and computer network is increasing, introducing new information warfare opportunities. The incidents and research discussed illustrate methods to exploit degrade, and possibly deny use of the mobile phone infrastructure or the devices themselves.

IV. Preliminary Research Results

This section provides the preliminary results of current research being conducted by the authors in addition to the analysis of incidents. Two sets of results are presented: a simulation analysis investigating jamming and eavesdropping in 3G mobile communications, and the results of interviews. Eavesdropping and jamming of wireless signals are tactics of electronic warfare; one of the functional areas of information warfare described above. The interviews results presented focus on the information warfare and security threats to the mobile networks.

A. Eavesdropping and Jamming of Mobile Phones

As the links to the end-user of the mobile phone networks is wireless, they are susceptible to interception and jamming. This section discusses some issues from previous research, and presents simulation results analysing potential effects of a specific attack on the wireless signal.

An issue with eavesdropping on mobile phones is that the base station controls the power with which the various mobile stations transmit in order to have the multiple user signals arriving at the base station with the same power; this results in an uneven distribution of signal power throughout the cell, which may be to the advantage or detriment of an eavesdropper [32]. Combined with the number of users in the cell, the eavesdropper should be located in close proximity to the target user; military electronic warfare equipment may be able to circumvent these issues. However, the encryption still will need to be broken.

Many devices are on the market which could be used to jam mobile phones in localised areas. These use signals that result in the mobile phones registering 'no signal'; these systems are effective for both GSM and 3G networks [33].

In 3G mobile communications, a spread-spectrum technology is used that employs the use of a unique spreading sequence that is used for both transmitting and receiving the signals; the correlation characteristics of the spreading sequence provides inherent security to the signals; primarily the signals are difficult to detect and have resistance to jamming. For more information on jamming of mobile phones see [34] and [35]. To circumvent this, a method of estimating the spreading code from the signal using an expectation-maximisation algorithm for the purposes of eavesdropping has been proposed [36]; this may also be extended to applications to improve jammer performance.

The estimated spreading sequence from the expectation-maximisation algorithm would need to be accurate; Monte Carlo simulations were performed using Matlab to illustrate the effects of the estimated sequence correlation with the actual sequence on performance, determined by the bit error rate (BER) at given signal-to-noise ratios (SNR) or jamming-to-signal ratios (JSR). The simulations comprised 100 iterations, and the data streams of 100,000 bits were randomly generated for each user. The channel noise was randomly generated additive white Gaussian noise at a SNR of 10dB; no other channel characteristics were modelled. Six users were modelled; all signals had equal strength at the receiver. Length-31 Gold codes were used for spreading sequences.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

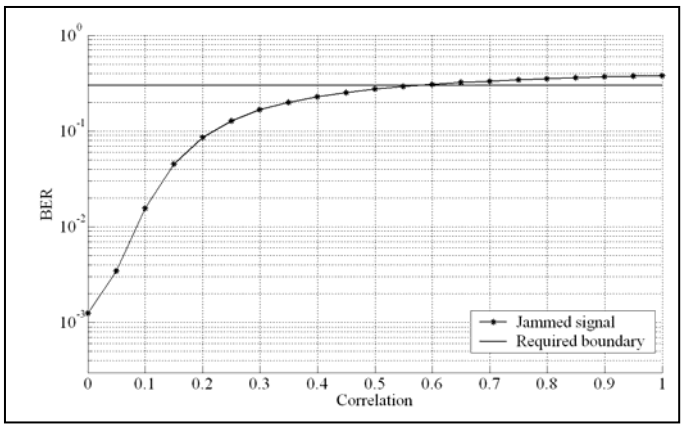

Figure 2. Signal performance under spread jamming

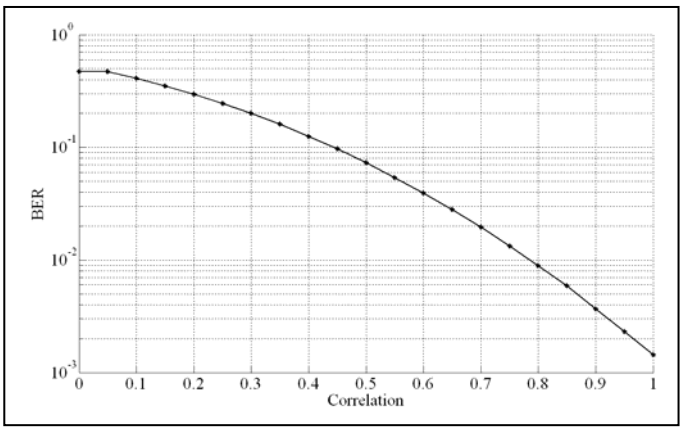

Figure 3. Performance of eavesdropping using estimated spreading code

For the jamming simulation, a JSR of 5dB at the receiver was used, and the jammer was considered as one of the six users. The results of the simulation are shown in Fig. 2. For digital signals, 20% of the signal needs to be jammed for the jamming to be effective, however 30% to 33% is usually taken as the correct figure [34, 35]. A 30% bound is shown in Fig. 2. As can be seen, a correlation of 0.6 is required for the jamming to be effective. At higher jamming-to-signal ratios this value of correlation will decrease.

The results of the eavesdropping simulation are shown in Fig. 3, and illustrate that very high correlation between the estimated sequence and real sequence is required to achieve reasonable performance. As the simulation assumed perfect power control, which is unlikely at an intercept receiver, and did not model channel characteristics such as fading, it can be assumed that actual performance would be worse, thereby requiring higher correlation.

For both the case of jamming and eavesdropping on the wireless channel, which are both electronic warfare attacks, the target area will be localised. Whilst sophisticated military and eavesdropping equipment are available and would probably give the required performance, a case can be made that the network warfare attacks to compromise the mobile switch centre will be more beneficial, as it gives access to a greater number of users, and can be controlled from anywhere in the world.

B. Results of Research Interviews

Interviews were conducted with international members of the information warfare, information security, and critical infrastructure protection communities; and the initial results are presented here. The purpose of the interviews is to get professional opinions on the importance of mobile phones, and the potential threats to the mobile infrastructure. Prospective respondents were identified through their publications; all respondents had either authored a book or report in the relevant subject areas. The e-Delphi method [37] was used, and five of six prospective responses were received. Three open-ended questions were asked relating to the security of the mobile phone infrastructure:

- What is the greatest information warfare or security threat to the mobile phone infrastructure?
- Should the cell phone infrastructure be considered part of the critical information infrastructure, and should cell phones be considered specifically in critical infrastructure and information security policies?
- How important are cell phones to the following: Large business; small business; military; government; security services; insurgents, terrorists, and criminals.

In response to the threats related to the mobile phone infrastructure, nine key terms were received, four of which related to access to information through monitoring. The five remaining concerns included: dependence, malware, cybercrime, lack of data verification, and the ability of smart phones to gain remote access with fewer security controls. This seems to indicate that there is a concern regarding the privacy of information on mobile networks, which is clearly understandable given the examples in section III.

There were four positive and one neutral response to the cell phone infrastructure forming part of the critical information infrastructure. Three positive, one neutral and one negative response were received regarding explicit critical infrastructure policies for mobile phones. These responses indicate that the mobile phone infrastructure should be considered as part of the critical information infrastructure, and there should be explicit consideration of the mobile phone infrastructure in the relevant policies.

Responses to the importance of mobile phones to various sectors were as follows: four positive and one neutral response were received for both small and large businesses; four positive and one negative response was received for government, military and security services. All the responses towards the importance of mobile phones to malicious actors (terrorists, insurgents and criminals) were positive. This illustrates the importance of the mobile phone infrastructure to a nation's wellbeing, and therefore it should be considered as part of the national critical information infrastructure. However, as mobile phones also have importance to malicious actors, countermeasures to mitigate exploitation, which may

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

include limited information warfare attacks on the infrastructure, should be made available.

The five international interviews discussed in this section do not provide sufficient results by themselves; additional interviews are to be conducted with local respondents to solicit information specific to South Africa. The interview results are to corroborate literature. In addition, a survey of informal traders in the major KwaZulu-Natal centres will be conducted to estimate the potential economic impact from this sector due to a severe outage of mobile services, which may occur due to a concerted information warfare attack on the information and communications infrastructure.

V. Conclusions

Information warfare may target information infrastructures through network warfare and electronic warfare in order to exploit, deny, degrade or corrupt information and the information infrastructure. The paper investigated significant information security breaches of the mobile infrastructure from an information warfare perspective.

The security incidents discussed show that the mobile infrastructure is a potential target for an information warfare attack; and there are potential vulnerabilities which could make the infrastructure susceptible to attack. Network warfare and electronic warfare attacks may be used to conduct information infrastructure warfare by exploiting and degrading or denying the services of the mobile phone infrastructure. From the examples and results presented, a network warfare attack, or using an insider, may prove to be more beneficial at a strategic level than an electronic warfare attack. Standard information security practices should mitigate the effects of such network attacks.

The results from the international interviews give an indication that there is some concern over the ease at which the confidentiality of the mobile infrastructure could be attacked. There is also an indication that the mobile infrastructure is important to national wellbeing, and should be explicitly considered as part of the critical information infrastructure.

References

[1] K. Van Rooyen, "Hidden price of a banking scam," The Sunday Times, pg. 9, 19 July 2009. (references)

[2] Unknown Author, "Call-hacking guide put on internet," The Daily News, pg. 4, 31 December 2009.

[3] K. Nohl, C. Paget, "GSM: srsly?" 26th Chaos Communications Congress, 27-30 December 2009, Berlin. Available at: http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf [Accessed 19 March 2010].

[4] W. Schwartau, "Cyberwar 4G," Infowarcon 2010, 12-14 May 2010, Washington D.C. Available at: http://www.crows.org/the-io-institute/infowarcon-2010-agenda.html [Accessed 25 June 2010].

[5] W. Hutchinson, and M. Warren, Information Warfare: Corporate Attack and Defense in a Digital World, Butterworth Heinemann: Oxford & Aukland, 2001.

[6] C. Kopp, "A fundamental paradigm of infowar," Systems, pp. 31-38, March 2000.

[7] D. Adamy, EW103: Tactical Battlefield Communications Electronic Warfare, Artech House: Boston & London, 2009.

[8] Global Mobile Suppliers Association, Evolution of Mobile Systems to 3G, 2010, available at: http://www.gsacom.com/news/statistics.php4 [Accessed 8 April 2010].

[9] W. Enck, P. Traynor, P. McDaniel, and T. La Porta, Exploiting open functionality in SMS-capable cellular networks, Proceedings of the 12th ACM Conference on Computer and Communications Security, Alexandria, pp. 393-404, 7-11 November 2005.

[10] D. Denning, Information Warfare and Security, Addison-Wesely: Boston, 1999.

[11] M. Brazzoli, "Future prospects of information warfare and particularly psychological operations," In: L. Le Roux (ed.), South African Army Vision 2020, Institute for Security Studies: Pretoria, 2007, pp. 217-232.

[12] J. Théron, "Operational battle space: an information warfare perspective," In: Phahlamohlaka, J. Veerasamy, N. Leenan, L. Modise, M. (eds.), IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace, CSIR: Pretoria, 2008, pp. 41-47.

[13] A. Jones, G. Kovacich, and P. Luzwick, Global Information Warfare, Auerbach Publications: Boca Raton, London & New York, 2002.

[14] M. Weaver, "Computer genius took hie revenge," The London Telegraph, 16 August 1999.

[15] V. Prevelakis, and D. Spinellis, "The Athens Affair," IEEE Spectrum, July 2007. Available at: http://spectrum.ieee.org/telecom/security/the-athens-affair/1 [Accessed 12 March 2010].

[16] S. Dingle, "Anatomy of an SMS banking scam," Fin24.com [online], 15 July 2009, Available at: http://www.fin24.com/articles/default/display_article.aspx?ArticleId=2638902 [Accessed 6 April 2010].

[17] S. Ragan, "GSM Alliance downplays seriousness of GSM project," The Tech Herald [online], 28 August 2009, available at: http://www.thetechherald.com/article.php/200935/4332/GSM-Alliance-downplays-seriousness-of-GSM-project [Accessed 6 April 2010].

[18] J Parial, An Analysis of the Cabir Mobile Phone Virus, CERT-In, 11 May 2005.

[19] F-Secure Corporation, F-Secure Virus Descriptions: Skulls.A [online], 9 November 2005, available at: http://www.f-secure.com/v-descs/skulls.shtml [Accessed 7 April 2010].

[20] F-Secure Corporation, F-Secure Virus Descriptions: Worm:SymbOS/Commwarrior [online], available at: http://www.f-secure.com/v-descs/commwarrior.shtml [Accessed 7 April 2010].

[21] C. Fleizach, M. Liljenstam, P. Johansson, G.M. Voelker, and A. Méhes, "Can You Infect Me Now? Malware Propagation in Mobile Phone Networks," *The 5th ACM Workshop on Recurring Malcode (WORM'07)*, Alexandria, Virginia, November 2007.

[22] R. Charette, "First Energizer, now Vodaphone: more malware found in store bought consumer electronic products," IEEE Spectrum Riskfactor Blog [online], 10 March 2010, available at: http://spectrum.ieee.org/riskfactor/computing/it/malware-found-in-store-bought-consumer-electronics [Accessed 6 April 2010].

[23] N. Seriot, "iPhone Privacy," Black Hat DC 2010, Arlington, Virignia, 2010. Availalble at: http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html [Accessed 26 June 2010].

[24] Unknown Author, "India Bans Chinese Cell Phones," StrategyPage.com, 2 May 2010, available at: http://www.strategypage.com/htmw/htiw/articles/20100502.aspx [Accessed 3 May 2010].

[25] A. Okeowo, "SMSs 'tool of hate in Kenya'," The Mail and Guardian, 19 February 2008, available at: http://www.mg.co.za/article/2008-02-19-smss-used-as-a-tool-of-hate-in-kenya [Accessed 4 March 2009].

[26] Unknown Author, "Gaza Cell Phones Targeted," Strategypage.com [online], 2 January 2009, available at: http://www.strategypage.com/htmw/htiw/20090102.aspx [Accessed 7 April 2010].

[27] L. Franics, "Phishing scams migrate to mobile," ITWeb [online], 23 July 2009, available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=24706:phishing-scams-migrate-to-mobile [Accessed 8 April 2010].

[28] J. Swartz, "Cell phones now richer targets for viruses, span, scams," USA Today [online], 28 April 2005, available at:

http://www.usatoday.com/money/industries/technology/2005-04-27-cell-phones-usat_x.htm [Accessed 8 April 2010].

[29] W. Knowler, "Be careful about what you're replying 'yes' to," The Daily News, pg. 10, 18 January 2010.

[30] R. Tate, "Apple's worst security breach: 114,000 iPad owners exposed," Gawker.com, 9 June 2010. Available at: http://gawker.com/5559725/att-fights-spreading-ipad-fear [Accessed 10 June 2010].

[31] C. Mulliner and C. Miller, "Fuzzing the phone in your phone," Black Hat USA 2009, 25 June 2009. Available at: http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html [Accessed 26 June 2010].

[32] A. McKellips and Sergio Verdu, "Multiuser detection for eavesdropping in cellular CDMA," Proceedings of the Asilomar Conference on Signals, Systams and Computers, vol. 2, pp. 1395-9, November 1997.

[33] R. Nichols and P. Lekkas, Wirelss Security: Models, Threats and Solutions, McGraw-Hill: New York, 2002.

[34] D. Adamy, EW103: Tactical Battlefield Communications Electronic Warfare, Artech House: Boston & London, 2009.

[35] R. Poisel, Modern Communications Jamming Principles and Techniques, Artech House: Boston & London, 2004.

[36] Y. Yao, and H.V. Poor, "Eavesdropping in the synchronous CDMA channel: an EM-based approach," IEEE Transactions on Signal Processing, vol. 49, no. 8, pp. 1748-1756, 2001.

[37] P. Lindqvist, and U. Nordanger, "Using the E-Delphi Method: An Attempt to Articulate the Practical Knowledge og Teaching," Journal of Research Methods and Methodilogical Issues, vol. 1, issue 1, 2007.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE