Vulnerability of South African Mobile Networks to Network Warfare Attacks

Brett van Niekerk and Manoj Maharaj
School of Management, IT, and Governance
University of KwaZulu-Natal
Westville, South Africa
991160530@stu.ukzn.ac.za

Abstract— **Web-based short messaging services and smart mobile devices susceptible to malware may provide attackers with tools to flood the mobile networks with illegitimate messages. Studies in the United States assessed the feasibility of web-based SMS denial-of-service attacks against the GSM mobile infrastructure. This paper repeats the study for the South African context, and simulation results are provided to model the traffic due to a rapidly propagating mobile worm infecting smart mobile devices. This indicates that the mobile phone infrastructure in South Africa is vulnerable to such attacks.**

Keywords- mobile phone infrastructure, network warfare, cyber warfare, information warfare

I. INTRODUCTION

In Africa there is a high penetration rate of mobile devices compared to the prevalence of fixed-line telecommunications; there is a ratio of approximately 11 mobile subscriptions for every fixed-line subscription for both voice and broadband [1]. This indicates that when considering the national critical information infrastructure, the mobile infrastructure in Africa can be seen to be more critical than in other nations with a more developed fixed-line telecommunications infrastructure [2]. As the mobile infrastructure forms part of the national infrastructure, its vulnerability to network warfare attacks needs to be assessed. This paper will focus on the particular case of denial-of-service attacks against the mobile infrastructure by overloading the wireless channels and infrastructure hardware with illegitimate SMS traffic. This expands on the research presented in [3-5], where the feasibility of network attacks on the mobile infrastructure was assessed. The previous research focuses on mobile infrastructures in the United States; this paper repeats the research for South Africa where relevant, and simulates the possible propagation of a hypothetical aggressive worm.

Section II provides the background to the mobile phone infrastructure, security concerns regarding smart mobile devices, and network warfare. Section III will discuss the calculations to determine the feasibility of attacks on the mobile infrastructure; both the previous research and the calculations for the South African scenario are provided. Section IV presents results of simulations into the propagation of a hypothetical mobile worm, and the impact on the mobile infrastructure components. Section V concludes the paper.

II. BACKGROUND THEORY

Here the background theory to the mobile phone infrastructure and its interconnections with fixed-line telecommunications and the Internet, security implications of smart mobile devices, and network warfare is presented.

A. Mobile Phone Infrastructure

This section presents an overview of the mobile phone infrastructure. The mobile stations (the devices) connect to the base station towers using wireless communications; in South Africa Global System for Mobile communications (GSM) and Wideband Code Division Multiple Access (WCDMA) are the main standards used [6]. This paper will focus on the GSM infrastructure. The base stations cover geographical areas called cells, hence the term cellular phones. Users are free to roam within that cell and between cells, and the most common reason for handover is to provide more efficient service due to the device moving [4, 26], however other criteria may also determine this. The wireless connection transmitting information from the base station to the mobile device is known as the downlink, and the connection transmitting from the device to the tower is called the uplink [7].

The mobile switching station is responsible for controlling the handoffs between the base stations, and connects to them with fibre-optic cables or wireless microwave links; they also connect the mobile infrastructure to the fixed-line telephone networks and other mobile networks [3]. The short messaging service centre is responsible for routing all SMS traffic, and external short messaging entities (EMSE) provide the capability of sending SMSs from the Internet or other external source to the mobile network [3]. The core of the mobile network consists of the home location register (HLR), visitor location register (VLR), the equipment identity register (EIR), and the authentication centre (AuC). The data network, specifically global packet radio service (GPRS), has additional components: the serving GPRS support node (SGSN) and the

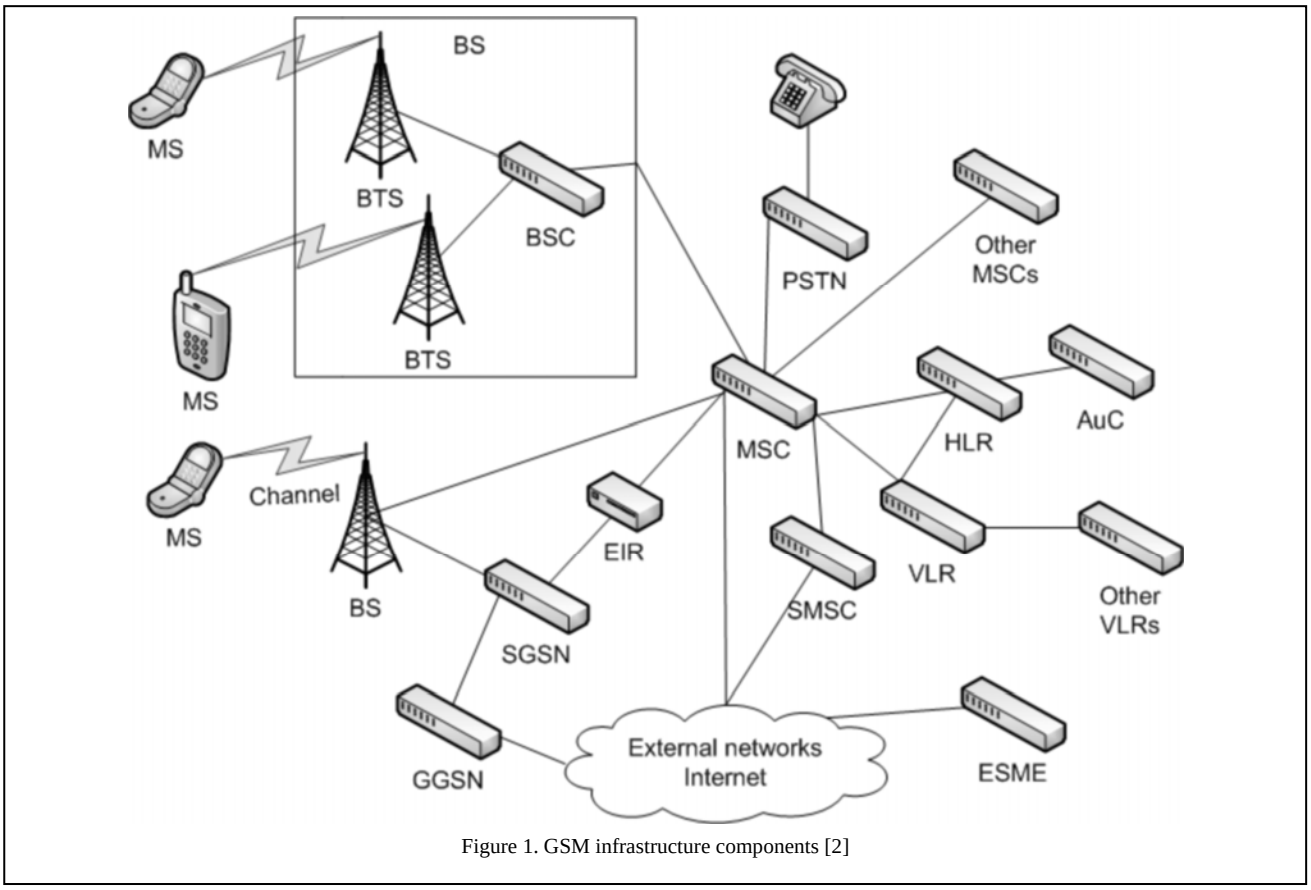

Figure 1. GSM infrastructure components [2]

gateway GPRS support node (GGSN) [8]. Figure 1 provides an overview of a mobile infrastructure. For the purposes of this paper, the focus will be on the HLR. It is responsible for the permanent information about the mobile users, which includes the billing information [8]. It is estimated that a single HLR controls 10 MSCs, and each MSC can control up to 200 BSCs [4]; this varies according to architecture and capacity, however this paper will use these figures to be consistent with previous research.

The wireless channels used for mobile communications are divided into two types: those for control and those to carry traffic [3]. Two control channels, the random access channel and paging channel, are used for initiating the services (both voice and data). The mobile devices are then instructed by the base station to monitor a stand-alone dedicated control channel (SDCCH) which is used for authentication and enabling encryption; it is also used for delivering SMS messages. Once the authentication is complete, a traffic channel is allocated for the mobile service (voice or data) [3]. The SDCCH is the channel to be considered in this paper.

B. Network Warfare

Network warfare, also known as cyber-warfare, is one of the functional areas of information warfare as defined by the South African National Defence Force, and its function is to attack an opponent's information networks while protecting one's own from attack [9, 10]. Network warfare may be used as a strategic weapon, and attack a nation's information networks and critical infrastructure on their home soil [11, 12]. For the purposes of this paper, the tactic of denying network resources and services will be considered; specifically those where the network is flooded by illegitimate traffic, preventing legitimate traffic from being processed. These denial-of-service (DoS) attacks may be achieved through rapidly propagating malware or configuring compromised systems to continuously transmit large volumes of traffic to flood the targeted network [13, 14].

C. Network Warfare and Security Considerations for Mobile Infrastructures

Mobile malware is a growing threat; whilst a major worm has not been seen on the mobile networks, one is expected [15]. Such a worm may have an impact on the mobile infrastructure equivalent to the SQL Slammer and Sasser worms that denied services on computer networks [2]. In 2009 an organised criminal group used an insider working for a South African mobile network provider to produce duplicate SIM cards, which was used to circumvent online banking security controls [16]. In Greece access was gained to a mobile network which gave the attackers remote control over the built-in eavesdropping hardware, enabling them to intercept communications with high-ranking individuals [17]. There are also reports that the Israeli military gained access to the mobile phone infrastructure in other nations, and left voice messages and sent SMSs [18]. These incidents illustrate that it is possible to gain access to the mobile infrastructure and remotely control certain aspects; it is feasible that similar attacks could be used

to flood the network with illegitimate traffic, denying legitimate communications.

The mobile telecommunications infrastructure can be considered as part of the national critical information infrastructure [2]. It can therefore be considered as a legitimate target for a network warfare attack, especially if the majority of the nation's telecommunications relies on the mobile infrastructure. In South Africa, there are approximately 10.9 subscriptions to mobile services for every fixed-line subscription (for both voice and data) [1, 2]; this indicates a reliance on this infrastructure.

The Minimum Essential Information Infrastructure lays out a series of vulnerabilities of information infrastructures. For the purposes of this paper only the following vulnerabilities will be considered [19]:

- Singularity and centralisation, where there is choke point or single point of failure;
- Sensitivity, where the infrastructure is sensitive to abnormal use or conditions;
- Capacity limits, where the infrastructure is operating at near capacity, making it vulnerable to DoS attacks;
- Electronic accessibility, where attackers can gain access remotely through electronic connections.

The network warfare attacks considered in this paper either employ electronic accessibility or malware on the devices to flood they network, thereby creating abnormal operating procedures that will either exploit the capacity limits of the wireless channels, or of key centralised components of the infrastructure, resulting in widespread failures.

III. CALCULATIONS

This section will discuss previous research assessing the ability of an attack on ESMEs being able to flood a mobile network with SMSs and deny legitimate traffic. As the SDCCH carries both SMSs and authentication information for voice services, by flooding the network with SMS traffic it may also be possible to deny voice services as they are unable to authenticate with the base station [3].

For each mobile carrier there are typically two SDCCHs per coverage sector; however, this may increase for densely populated areas, which will have more carriers or SDCCHs per sector. Each SDCCH can carry approximately 900 SMSs per hour [3]. The following equation can be used to calculate the capacity C of mobile networks in a given populated geographical area [2, 3]:

$$C = (\text{no. sectors}) \times (\text{SDCCHs/ sector}) \times (\text{SMS/sec/SDCCH}) \quad (1)$$

It is estimated that an SMS uses 1500 bytes to be transmitted over the internet; this includes the web page, the traffic overhead, and the characters of the SMS itself. The SMS characters are typically 160 bytes [3]. This can then be used to determine the Internet bandwidth required to transmit sufficient illegitimate SMSs to flood the targeted mobile networks.

Section A presents the original results that focus on the United States. Section B will present the results for four South African metropolitan areas.

A. *Previous Results - United States*

The original results were for two cities in the United States: Washington, D.C. and Manhattan. The capacity was calculated for various numbers of SDCCH channels per coverage sector. The required bandwidth was then calculated for using individual messages, or having ten recipients per message [3]. Table I shows these results.

It was estimated that a SMSC in 2000 could process 2500 SMSs per second [3]; therefore the number of SDCCHs could treble without the SMSC reaching its capacity. This indicates that the volume of traffic required to overload the control channels in a specific city is realisable. The required bandwidth is for the internet connection is also small and realisable.

The total number of messages required to overload the entire United States mobile infrastructure was calculated as 325 525 messages per second. This translates to approximately 3.8 Gbps, or 370 Mbps if each SMS is sent to ten recipients [3]. Given that a distributed denial-of-service (DDoS) attack against Burma in 2010 approached 14 Gbps [20], the required traffic to theoretically overload the entire United States mobile infrastructure is feasible.

B. *South Africa*

The study above was redone for the case of four South African metropolitan areas: Cape Town, eThekwini (Durban), Johannesburg, and Tshwane (Pretoria). From the above study, the average size of a coverage sector was 0.5 mi^2 to 0.75 mi^2 [3], this equates to 1.3 km^2 to 2 km^2. Table II shows the

TABLE I. CAPACITY AND BANDWIDTH FOR DOS ATTACK ON US MOBILE NETWORKS [3]

City	Area	Sectors	SDCCH/sector	SMS Capacity (SMS/sec)	Upload Bandwidth (kbps)	Multi-recipient bandwidth (kbps)
Washington D.C	68.2 mi^2	120	8	240	2812.5	281.25
			12	360	4218.8	421.88
			24	720	8437.5	843.75
Manhattan	31.1 mi^2	55	8	110	1289.1	128.91
			12	165	1993.6	193.66
			24	330	3867.2	386.72

TABLE II. NUMBER OF SECTORS FOR CITIES [2]

Metropolitan area	Area (km^2)	No. of Sectors	
		1.3 km^2	*2 km^2*
eThekwini	2291	1762	1146
Cape Town	2460	1892	1230
Johannesburg	1644	1265	822
Tshwane	2147	1672	1087

calculations to estimate the number of sectors per metropolitan area.

For the purposes of this paper, the worst case scenario from the perspective of the attacker will be considered; the feasibility of these scenarios indicates the other scenarios are also feasible. Therefore the most number of sectors will be taken for each city, indicating more SDCCHs and therefore a higher capacity to carry messages. South Africa has three main network providers (MTN, Vodacom, and Cell C); recently Telkom introduced a mobile network (8ta), and there is a virtual network provider (Virgin). The SMS capacity will be calculate for two and three SDCCHs per sector for the three main network providers (giving six and nine SDCCHs per sector) and for the three main providers with the two other network providers (giving 10 and 15 SDCCHs per sector). The SMS capacity is calculated and shown in Table III.

TABLE III. MESSAGE CAPACITY (SMS/SEC) [2]

Metropolitan area	SDCCHs per Sector			
	6	*9*	*10*	*15*
eThekwini	2643	3964.5	4405	6607.5
Cape Town	2838	4257	4730	7095
Johannesburg	1897.5	2846.3	3162.5	4743.8
Tshwane	2508	3762	4180	6270

From these results, the maximum capacity is 7095 SMS/sec; when the message rate reaches this capacity the infrastructure performance will be severely degraded due to the channel being saturated. Messages may also create a backlog and continue to disrupt services after the actual active attack has ceased [2]. This is similar to the Blackberry outages in 2011; after the initial outages it was reported that message backlogs still overwhelmed the servers, resulting in problems with delivering the services [21]. A mobile infrastructure operating close to its capacity limits will be more susceptible to attacks; smaller attacks may increase the total number of messages over the capacity limit and begin to disrupt services [2]. In South Africa, there have been reports of poor mobile service delivery due to the mobile infrastructure operating at high capacity [22, 23]; this indicates that the mobile infrastructure in South Africa may be vulnerable to a DoS attack.

Table IV presents the Internet bandwidth required to conduct such a DoS attack on the South African mobile infrastructure through the Internet. The maximum required bandwidth is for Cape Town, requiring 81.2 Mbps. However, the three digit prefix of South African mobile phone numbers are not arranged by geographical area as in the United States, but according to the network provider; therefore it will be difficult to target a specific city [2, 6]. Taking the total bandwidth requirements for the four largest metropolitan areas, it can be estimated that a bandwidth of 282.9 Mbps is required to severely degrade the mobile services in South Africa [2]. As the Burma attacked reached 14 Gbps, generating this bandwidth is feasible. Currently, the active undersea cables off the African coast that land in South Africa have an estimated capacity of over 9000 Gbps [24], indicating that this traffic can reach the country. A possible limitation to this type of attack is the capacity of the ESMEs to transmit the required messages [2].

TABLE IV. BANDWIDTH REQUIREMENTS (Mbps) [2]

Metropolitan area	SDCCHs per Sector			
	6	*9*	*10*	*15*
eThekwini	30.2	45.4	50.4	75.6
Cape Town	32.5	48.7	54.1	81.2
Johannesburg	21.7	32.6	36.2	54.3
Tshwane	28.7	43.1	47.8	71.8

This section indicates that a DoS attack against the South African mobile infrastructure is feasible; the required bandwidth to generate the required messages to saturate the infrastructure is achievable, and the undersea cables connecting South Africa to the global information infrastructure can carry the required traffic. Reports of service disruptions in the South African mobile infrastructure indicate that there may be a susceptibility to a DoS attack. The following section provides simulations of an aggressive mobile worm propagating through the mobile networks, and its potential impact on the mobile infrastructure.

IV. SIMULATIONS

This section presents results from simulations of a hypothetical mobile worm that propagates aggressively through the mobile network. Previous research indicated that 23 500 to 141 000 infected mobile devices making malicious requests would be able to reduce the capacity of HLRs to carry legitimate traffic by 75% [4]. Other research conducted simulations to investigate the effect of address book topology and wireless link capacity on the ability of the malware to propagate via MMS or over and voice over IP networks [5]. The simulations presented here investigate the time taken for the infrastructure hardware to become saturated.

The simulations will be based on the Beselo worm; however, more aggressive propagation characteristics will be used. The Beselo worm propagated by MMS by sending infected messages to the entire contact list of the device every two minutes [25]. For the purposes of these simulations, the hypothetical worm attempted to propagate every minute. The total number of infections is limited to a specific population size. The populations of the four metropolitan areas in

considered above range from just over two million for Pretoria to 3.3 million for Johannesburg, with both Durban and Cape Town at approximately three million. For the simulation, it was assumed that 1% of the population in the metropolitan areas would have devices that could be infected; therefore the population limit was set at thirty thousand.

The propagation of the worm was modelled using two interdependent mathematical sequences; one provided the number of infected devices, and the second provided the number of devices transmitting the infected message. The number of transmitting devices at a point in time was determined by the sequence of infected devices for previous points in time. The number of infected devices at a specific point in time was determined by the number of transmitting devices at previous points in time limited by various factors. These factors include the percentage of the total device population that could be infected, which was scaled down using the random number generating function in Matlab. Other factors influencing the propagation was the capacity and loading on the infrastructure hardware. The settings for the plots in Figures 2 and 3 are as follows:

- Total population of 30 000;
- One initial infection;
- Five SMSCs each with a capacity of 2500 msgs/sec;
- An address book size of 100.

Figure 2 shows the increase over time of the infected devices and devices transmitting the malicious messages for various existing loads on the mobile infrastructure. Figure 3 shows the number of malicious messages processed or rejected by the infrastructure components for the various loads.

The propagation of the worm is hindered for higher existing loads on the infrastructure as these messages form a lower percentage of the total traffic, therefore the likelihood that the malicious infections are successfully processed and then infect another device decreases. This can be seen due to the number of messages processed for a 75% existing load in Figure 3.

Table V provides the time taken from the first infection until the networks become saturated with malicious messages. These times are for various existing network loads, numbers of initial infections, and populations. As above, five SMSCs are assumed, each with a capacity of 2500 msgs/sec; the address book size is assumed to be 100 entries.

The worst case for the attacker, namely a small population and only one initial infection, will take an estimated 45.4 minutes to severely degrade the network capacity to the point where it drops many messages. By increasing the number of initial infections, the propagation of the worm is much quicker [2]. Table V indicates that the higher the existing load, the sooner the network becomes saturated. This is as expected, however this scenario also inhibits the worm's ability to propagate, as discussed above.

Previous research showed that 11 750 infected devices would be required to degrade a HLR's ability to process legitimate requests by 90% in a metropolitan area [4]. Given Figure 2 and Table V, this can be achieved within an hour even if the capacity of the HLRs is doubled. Higher capacity HLRs may require 141 000 infected devices [4]; this will be

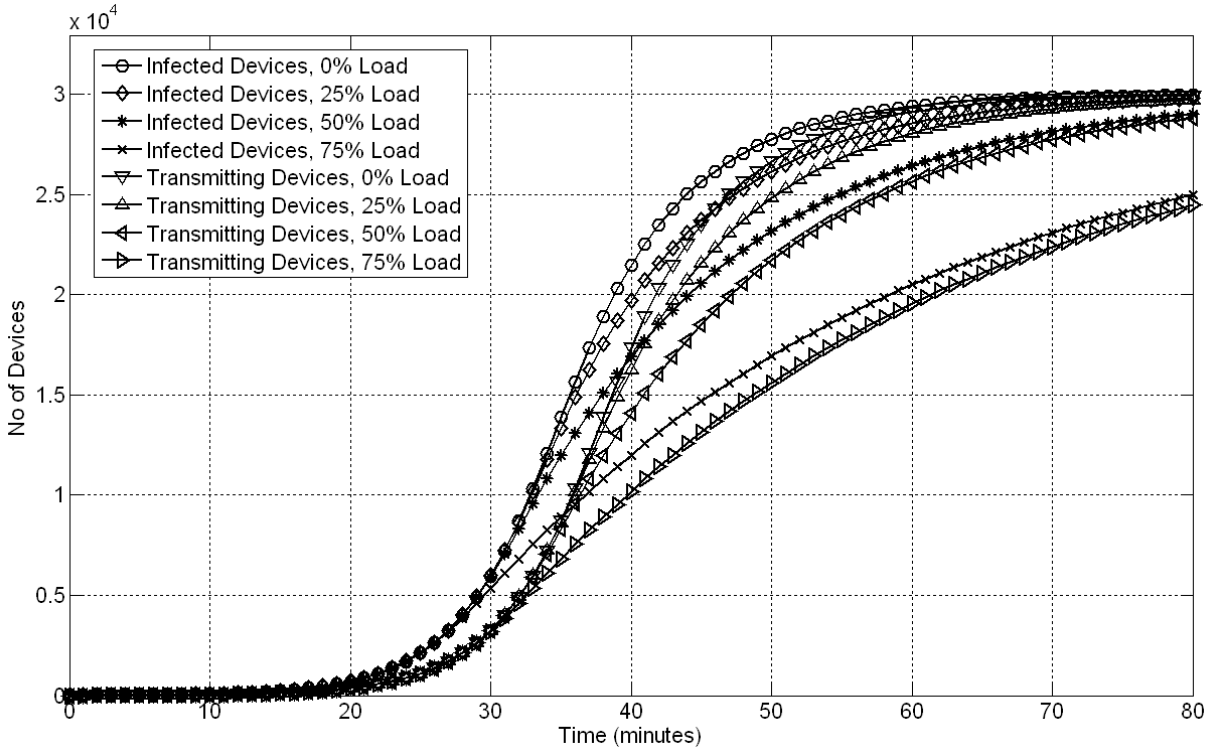

Figure 2. The Increase in Infected and Transmitting Devices over Time [2]

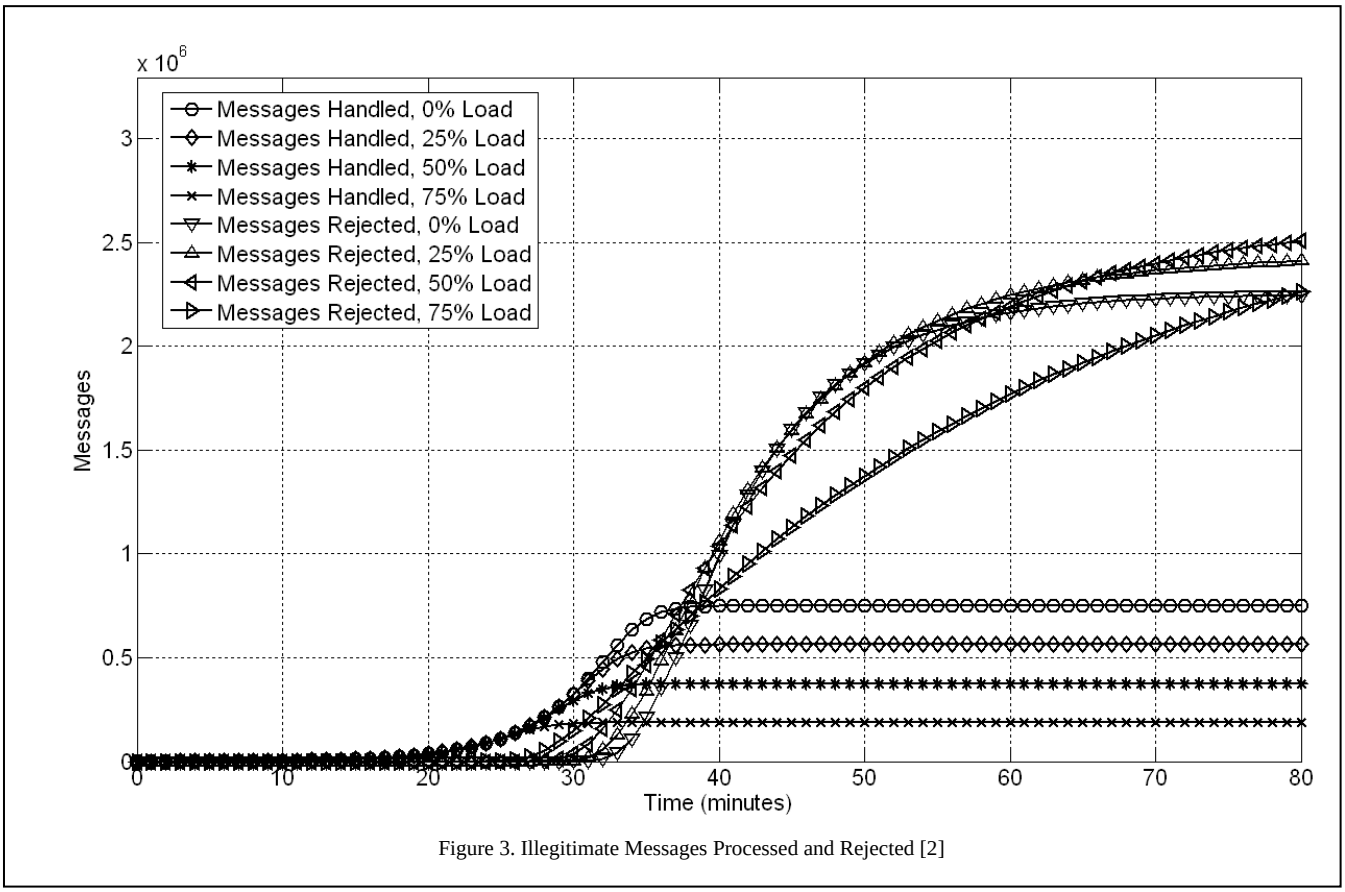

Figure 3. Illegitimate Messages Processed and Rejected [2]

achievable at a national level given a population of 45 000 devices that can be infected in each of the four major population areas. Therefore if the SMSCs and channels can cope with the traffic of generated by the worm's propagation, the HLRs may fail. This results in three layers of vulnerability: the channels, the SMSCs, and the HLRs. The attack only needs to overcome one layer to succeed.

Countermeasures to such attacks include firewalls and anti-spam filters for SMS services. These can be used to prevent malicious messages from entering the network [27, 28], or mobile security software protects individual devices by filtering out malicious messages [29, 30]. Security software installed on mobile phones may reduce the chance of the device becoming infected, and by blocking malicious messages it hinders the worm's ability to propagate.

V. CONCLUSIONS

The mobile infrastructure in South Africa can be considered critical due to the reliance on mobile communications over traditional fixed-line telecommunications. Reports of service disruptions due to high operating loads indicate that the infrastructure may be susceptible to DoS attacks. This paper assesses the feasibility of such attacks. The study is limited in that it replicates a study that is dated. It is intend to include

TABLE V. TIME TO NETWORK SATURATION (MINUTES) [2]

Population	Initial Infections	0% Load	25% Load	50% Load	75% Load
15000	1	45.4	43.8	41.4	37.8
	5	38.1	36.3	34.0	30.6
	10	34.9	33.1	30.9	27.5
30000	1	44.6	43.1	41.0	37.8
	5	37.2	35.7	33.6	30.4
	10	34.1	32.4	30.6	27.4
45000	1	44.4	43.0	41.0	37.8
	5	37.1	35.4	33.6	30.3
	10	33.9	32.3	30.4	27.2

modern mobile infrastructure architectures and capacity limitations in future research.

From the calculation, the total bandwidth required to generate the required SMSs to degrade mobile services nationwide through compromising ESMEs over the Internet is estimated to be 282.9 Mbps. This is considered achievable by comparing it to the known traffic rate of DDoS attacks and the capacity of the undersea cables along the African coast.

The simulations to investigate the effects of an aggressive mobile worm propagation on a mobile network estimates that the mobile infrastructure will experience severe degradation of its capacity within an hour. Given the concerns over the high operating loads of the South African mobile infrastructure [22, 23], this indicates that it will be vulnerable to such DoS attacks, which could deny mobile communications.

ACKNOWLEDGEMENTS

This paper is published from the first Author's PhD Thesis. The PhD was supported by grants from South African Department of Defence, and the Armscor Ledger Program through the Cyber Defence Research Group at the Council for Scientific and Industrial Research, Defence, Peace, Safety and Security (CSIR-DPSS), and the University of KwaZulu-Natal.

REFERENCES

[1] International Telecommunications Union, ICT Data and Statistics, 2011. Available at: http://www.itu.int/ITU-D/ict/statistics/index.html

[2] B. van Niekerk, Vulnerability Assessment of Modern ICT Infrastructure from an Information Warfare Perspective, PhD Thesis, University of KwaZulu-Natal, 2012.

[3] 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.

[4] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, et al., "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core," Proceedings of the 16th ACM Conference on Computer and Communications Security (CSS '09), Chicago, pp. 223-234, 9-13 November 2009.

[5] 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.

[6] B. van Niekerk, and M. Maharaj, "Mobile Security from an Information Warfare Perspective," Information Security South Africa 2010, Sandton, 2010.

[7] T. Ojanpera, and R. Prasad, Wideband CDMA for Third Generation Mobile Communications, Artech House: Boston and London, 1998.

[8] C. Xenakis, and L. Merakos, "Vulnerabilites and Possible Attacks against the GPRS Backbone Network," Critical Information Infrastructures Security, Springer: Samos, Greece, 2006 , pp. 262-272.

[9] 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.

[10] 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.

[11] R.C. Molander, A.S. Riddile, and P.A. Wilson, Strategic Information Warfare: A New Face of War, RAND Institute: Santa Monica, 1996.

[12] R.C. Molander, P.A. Wilson, D.A. Mussington, and R.F. Mesic, Strategic Information Warfare Rising, RAND Institute: Santa Monica, 1998.

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

[14] T.R. Peltier, J. Peltier, and J. Blackley, Information Security Fundamentals, Auerbach Publications: Boca Raton, London, and New York, 2005.

[15] M. Hyppönen, F-Secure Mobile Security Review September 2010, FSecure News You Tube Channel [online], 11 October 2010, available at: http://www.youtube.com/watch?v=fJMLr8BDQq8 [Accessed 13 December 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] 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].

[18] 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].

[19] R.H. Anderson, P.M., Feldman, S., Gerwehr, B., Houghton, R., Mesic, J., Pinder, et al., Securing the US Defense Information Infrastructure: A Proposed Approach, RAND Institute: Santa Monica, 1999.

[20] C. Labovitz, "Attack Severs Burma Internet," Arbour Networks [online] November 2010. Available at http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/ [Accessed 11 November 2010].

[21] Press Association, "BlackBerry Users Vent Frustrations on Third Day of Service Disruption," The Guardian, 12 October 2011. Available at: http://www.guardian.co.uk/technology/2011/oct/12/blackberry-service-disruption-third-day [Accessed 13 October 2011].

[22] K. Ajam, and C. Bailey, "Cellphone Chaos Fears," The Independent on Saturday, 30 May 2009, p. 1.

[23] South African Press Association, "ICASA: Cell Operators Don't Meet Requirements," Daily News, 1 July 2011. Available at: http://www.dailynews.co.za/icasa-cell-operators-don-t-meet-requirements-1.1092245 [Accessed 3 July 2011].

[24] S. Song, "African undersea cables," *Many Possibilities* [online], 2010. Available at: http://manypossibilities.net/african-undersea-cables/ [Accessed 19 November 2010].

[25] Cisco, Cisco 2008 Annual Security Report, 2009. Available at: http://www.cisco.com/en/US/prod/collateral/vpndevc/securityreview12-2.pdf [Accessed 24 January 2011].

[26] UMTSWorld.com, "UMTS handover," *UMTS World* [online], 2003. Available at: http://www.umtsworld.com/technology/handover.htm [Accessed 5 July 2012].

[27] CM Telecom, "SMS Firewall," CMTelecom.com [online], 2011. Available at: http://www.cmtelecom.com/application/sms-firewall [Accessed 5 July 2012].

[28] Tekelec, "SMS Firewall," Tekelec.com [online], 2012. Available at: http://www.tekelec.com/products/sms-firewall.asp [Accessed 5 July 2012].

[29] Kaspersky, "Kaspersky Mobile Security," Kaspersky.com [online]. 2012. Available at: http://www.kaspersky.com/kaspersky_mobile_security [Accessed 5 July 2012].

[30] Symantec, "Norton Smartphone Security," Norton Security Store [online], 2012. Available at: http://www.norton-security-store.com/symantec-norton-software-abstracts/norton-smartphone-security.html [Accessed 5 July 2012].