REMARKS ON CYBERSECURITY SYMPOSIUM
By David Mahlobo MP, Minister of State Security
SUNDAY 01 MARCH 2015, SANDTON

Programme Director
The Event Organisers
Senior Government Officials
Leadership of Business
Leadership of Academia
Sponsors
Distinguished guests,
Media Houses
Comrades and Friends
Ladies and gentlemen

Introduction

1. It is a great honour and a real pleasure to address this gathering. Let me also express my thanks to the organizers and sponsors for making this 1st SA Cybersecurity Symposium a reality.

2. Today I was amongst many South Africans who joined HE President Zuma in a service on the arrival of the mortal remains of forebears, revolutionaries and the architects of this democratic South Africa, JB Marks and Moses Kotane.

3. Our sincere gratitude and congratulations to our President for making this day a reality.

4. We can boldly say we are Free at Last through the ultimate premium Marks, Kotane and other generations had to pay for our hard fought free. We owe to them to continue to build a national democratic society as envisioned sixty years ago in Kliptown.

5. Through our vision for the future, the freedom charter, we declared: *"South Africa belongs to all who live in it black and white; no government can claim authority unless it is based on the will of the people….we pledge ourselves to strive together, sparing neither strength nor courage until the democratic changes here set out have been won.*

6. Let's celebrate our achievements over the last 21 years of our freedom. As South Africa and her people we are on track in building a truly united, non-racial, non-sexist, democratic society but we are the first to admit that more still needs to be done.

7. Ladies and gentlemen, personal privacy and national security in the 21st century both depend on protecting a set of systems that didn't even exist until late 20th century. The advent of the electronic web of information-sharing known as cyberspace has revolutionized the world. It has brought exciting opportunities in developing our economies, improving our health care, education, agricultural production, military, provision of services etc. These opportunities are endless.

8. In the same vein, electronic computing and communication pose some of the most complex challenges the world has ever faced. They range from protecting the confidentiality and integrity of transmitted information and deterring identity theft to preventing the scenario recently dramatized in the Bruce Willis movie *"Live Free or Die Hard,"* in which hackers take down the transportation system, then communications, and finally the power grid.

9. As that movie depicted, networks of electronic information flow are now embedded in nearly every aspect of modern life. From controlling traffic lights to routing airplanes, computer systems govern virtually every form of transportation.

10. Radio and TV signals, cell phones, and (obviously) e-mail all provide vivid examples of how communication depends on computers — not only in daily life, but also for military, financial, and emergency services. Utility systems providing electricity, gas, and water can be crippled by cyberspace disruptions. Attacks on any of these networks would potentially have disastrous consequences for individuals and for society.

11. In fact, serious breaches of cybersecurity in financial and military computer systems have already occurred. Identity theft is a burgeoning problem. Viruses and other cyber-attacks plague computers small and large and disrupt commerce and communication on the Internet.

12. Yet research and development for security systems has not progressed much beyond a strategy akin to plugging the hole in the dike — cobbling together software patches when vulnerabilities are discovered.

13. Historically, the usual approach to computer protection has been what is called “perimeter defence.” It is implemented by placing routers and “firewalls” at the entry point of a sub-network to block access from outside attackers.

14. Cybersecurity experts know well that the perimeter defence approach doesn’t work. All such defences can eventually be penetrated or bypassed. And even without such breaches, systems can be compromised, as when flooding Web sites with bogus requests will cause servers to crash in what is referred to as a “denial of service” attack or when bad guys are already inside the perimeter.

15. The problems are currently more obvious than the potential solutions. Any country or enterprise need to better mitigate and defend against dynamic threats, minimizes risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

16. We need to work hard in terms of research to develop innovations for addressing a long list of cybersecurity priorities. For one, better approaches are needed to authenticate hardware, software, and data in computer systems and to verify user identities. Biometric technologies, such as fingerprint readers, may be one step in that direction that has been introduced in our own country

17. A critical challenge for all nations is more about securing the software. One way to do this may be through better programming languages that have security protection built into the ways programs are written. And technology is needed that would be able to detect vulnerable features before software is installed; rather than waiting for an attack after it is put into use.

18. Another challenge is providing better security for data flowing over various routes on the Internet so that the information cannot be diverted, monitored, or altered. Current protocols for directing data traffic on the Internet can be exploited to make messages appear to come from someplace other than their true origin.

19. To achieving integrity and securing our cyber space must be accompanied by methods of monitoring and quickly detecting any security compromises. The ability to detect malicious activity and disable attempted intrusions automatically. And then once problems are detected, technologies for taking countermeasures and for repair and recovery must be in place as well.

20. Part of that process should be new forensics for finding and catching criminals who commit cybercrime or cyberterrorism.

21. As people we must recognize that a cybersecurity system's success depends on understanding the safety of the whole system, not merely protecting its individual parts. Consequently cybercrime and cyberterrorism must be fought on the personal, social, and political fronts as well as the electronic front.

22. More research is needed on how people interact with their computers, with the Internet, and with the information culture in general. Cultural and social influences can affect how people use computers and electronic information in ways that increase the risk of cybersecurity breaches.

23. It would also be helpful to gain a better understanding of the psychology and sociology that leads to deliberate computer crime. Systems must be secure not just against outsiders, but also against insiders who might sabotage a system from within.

24. Laws and regulations concerning cybersecurity need to be evaluated for their influence on how people use or misuse electronic information. And perhaps most important, political forces need to be marshalled to support and fund the many lines of research that will be needed to accomplish the complex task of protecting cyberspace from attack.

25. South Africa and Africa's ICT sector has experienced extraordinary growth in recent years, especially in terms of mobile cellular communications.

26. The growing use of smart phones and other mobile devices to access the Internet has seen more consumers increasingly vulnerable to cybercrime as they enter the cyber space with little or no Cybersecurity awareness.

27. In recent years, we have seen an enormous increase in the usage of social media networks. Social media networks have the power to help people voice their demands and mobilize their forces. We all know in the case of the so-called *Arab Spring* how people mobilised themselves or were mobilised to effect a regime change through social media. Having said that, two-thirds of the world's population is currently not online and it should be our desire as a nation to make ICTs accessible to give people the power to transform their lives through education, health care and everything else the online world offers.

28. We take cognizance of the fact that the borderless nature of cyber space, the emergence of social networks and mobile phone platforms offer vast opportunities for innovation, competitiveness, economic growth, digital integration, education and citizens' participation in governance. At the same time inter-connectedness potentially threatens on an unprecedented scale the opportunity for cyber related attacks against countries, organisations and individuals. The exploitation of ICT's

vulnerabilities creates new threats and ever-growing challenges globally, raising new challenges for national and international security structures.

29. Ladies and Gentlemen, you are well aware of the various scams and fraudulent activities undertaken by cybercriminals and syndicates to get to your personal information and financial data.

30. Whilst in other instances security breaches may be attributed to negligence in protection of information, corporate espionage by competitors and hackers, disgruntled employees pose even a bigger threat as in the case of a former Gautrain contractor who hacked into the system some weeks ago after being fired and attempted to steal about R800 million.

31. The Hawks foiled the plan and nabbed the implicated perpetrator. It is alleged that he is linked to the well planned and executed bank heist in 2012 which set Postbank R42m off.

32. The Hawks also foiled a plan by two Eskom employees to steal millions of rands by hacking into the utility’s payroll system.

33. Ladies and Gentleman, Cybercrime affects everyone, Governments, business and individuals alike. Globally, nation States are faced with a challenge of putting measures in place to protect their territorial integrity, national security and critical infrastructures and citizens against cyber-attacks, cyber terrorism and cyber warfare.

34. Experts tell us that SA has lost R5bn in hack attacks in 2014, warning Businesses to take heed as cybercrime is on the increase in South Africa. This figure can be higher as there are no exact cybercrime figures available.

35. Companies opt to keep quiet about breaches as the reputational damage companies faced could take them out of business.

36. It is a worrying fact to share that, cyber criminals and syndicates are highly skilled, highly trained and their aim is long-term attacks and staying hidden on networks for extended periods of time. Government is committed to building capacity and implementing measures to stay ahead of cyber criminals and call upon private sector to join hands with Government to fight this.

37. The Government's approach in dealing with this matter is premised on the policy principle that National security, which includes the security of the Information and Communications Technologies in the country, is a responsibility of the structures responsible for security in the Republic. Government at the same time acknowledges the role of the private sector and the general public as the critical stakeholders in ensuring the secure use of ICTs.

38. Our view is that this situation also exposed us to exploitation by enemies of the State as it is common practice internationally for foreign ICT vendors to deploy ICT Security solutions that have backdoors. This enables their intelligence agencies to have unauthorized access to critical information systems.

39. Significant strides are being made in enhancing the security of the nation's critical physical infrastructure as well as its cyber infrastructure and networks. Today's threats to cybersecurity require the engagement of the entire society—from government and law enforcement to the private sector and importantly, members of the public—to block malicious actors while bolstering defensive capabilities.

40. We have improved our laws to deal with the emerging threats and opportunities in the cyber space like, Electronic Communications and Transactions Act no 25 of 2002 (ECT Act); Electronic Communications Security (Pty) Ltd Act no 68 of 2002 (COMSEC ACT) and Amendments to SITA Act no 88 OF 1998 (SITA Act).

41. These Acts were passed in recognition of the various roles that State entities can play in relation to securing South Africa’s Critical Communications and Critical Information Infrastructures. The ECT Act was intended to deal with, amongst others, the facilitation and regulation of the electronic communications and transactions in the country which would include the development

of a national Electronic Communications Strategy, National E-Government services and the protection of what is referred to as the critical databases in the Republic.

42. The State Security Sector through NIA at the time initiated a process for the enactment of the Comsec Act so as to establish a State entity with a responsibility for the protection and securing of Critical Information Infrastructure of Organs of State. The Act envisaged a situation where the Minister for Intelligence would prescribe those communications that are critical for the political, social and economic well-being of the Republic. The Act required that those technologies be identified and protected at the State's expense.

43. In March 2012, Cabinet approved a National Cybersecurity Policy Framework (NCPF) which seeks to, amongst others, deal with the following:

a. Centralize coordination of Cybersecurity activities within SA so as to have a coordinated approach to cybercrime, national security imperatives and enhance the information society and knowledge based economy;

b. Strengthen intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;

c. Anticipate and confront emerging cyber threats, in particular threats to National Critical Information Infrastructure and coordinate responses thereto;

d. Foster cooperation and coordination between Government, the private sector and civil society including ensuring that South Africa becomes a critical contributor to international cooperation on Cybersecurity matters.

e. Develop skills, Research and Development capacity, promote Cybersecurity culture and promote compliance with appropriate technical and operational Cybersecurity standards.

44. A National Cybersecurity Policy Framework implores us to work collaboratively with public, private, and international entities to protect infrastructure, enhance situational awareness and implement analysis, warning and risk-management programs.

45. To ensure greater cooperation and national alignment of the implementation process, the Cybersecurity Response Committee (CRC), a strategic body chaired by SSA, responsible for Cybersecurity priority setting and overseeing the implementation of the NCPF was established.

46. We need to build more partnerships if we are to succeed. Our capacity to respond is depend on systems and human capital development.

47. Working with universities and other research institutes to build the cybersecurity pipeline through competitive scholarship, fellowship, and internship programs must be our preoccupation to attract top talent and develop systems that have command and control in our hands, national sovereignty.

48. It is our duty led by government to guide research and development as well as advancements in scientific and technical knowledge to support cybersecurity through targeted grant programs that encourage academic research, private sector investment, and innovation from small businesses.

49. We believe that Academic institutions should take a lead in developing academic programs that focus on developing the required technical skills in partnership with Government. This should include an engagement on appropriate curriculum with relevant State entities. We strongly believe that this focus will assist South Africa in ensuring that students are channelled to courses that develop this capacity for the country.

50. The private sector is expected to contribute to national skills, research and development. The private sector is expected to implement information security standards and contribute to the protection of National Critical Information Infrastructures.

51. In our efforts are to be sustainable, we should underscore public cybersecurity awareness campaign is designed to increase public understanding of cyber threats and promote simple steps the public can take to increase their safety and security online.

52. The civil society is expected to take interest in the general awareness programs and at least ensure their devices have updated malware protection. To this end, Government will run cybersecurity awareness programmes to raise the level and capacity of end users to use ICTs responsibly.

53. To give effect to the NCPF, Government has drafted various policies, strategies and reviewed existing laws to determine adequacy in dealing with cyber challenges in the country.

54. To this end, a draft Bill was developed under the leadership of the Department of Justice and Constitutional Development in line with their mandate. In the coming months, we will be engaging industry and the public at large to get inputs on these draft documents.

55. We look forward to a fruitful engagement and urge you all to take keen interest in this work so as to build a better and safe cyber space for all. It is also clear that with greater cooperation by all stakeholders, we will be able to move the ICT sector forward

56. Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all.

57. Securing our cyberspace will ensure conditions for peace, security and development are enhanced.

58. As conclude let me indicate that our country led by HE President Zuma will leave no stone unturned in delivery on our promise. We shall ensure that this country's sovereignty, her people, infrastructure and interests are protected.

59. In closing let me once again reiterate the vision of the Freedom Charter, Let all who love their people and their country now say, as we say here: "***THESE FREEDOMS WE WILL FIGHT FOR, SIDE BY SIDE, THROUGHOUT OUR LIVES, UNTIL WE HAVE WON OUR LIBERTY"***

60. Inde lendlela esihambayo!!!

61. I wish you a successful conference.

62. I thank you.