

A decorative graphic on the left side of the slide consists of a network of thin, light blue lines. These lines form a complex, branching pattern that resembles a circuit board or a neural network. Some lines end in small circles, while others are open. The overall effect is a modern, technological aesthetic that complements the title's focus on cyber space.

DETERMINANTS OF SOUTH AFRICA'S FOREIGN POLICY STRATEGY IN CYBER SPACE

LAURENCE CAROMBA, MONASH SOUTH AFRICA

9 MAY, 2009: SOUTH AFRICA

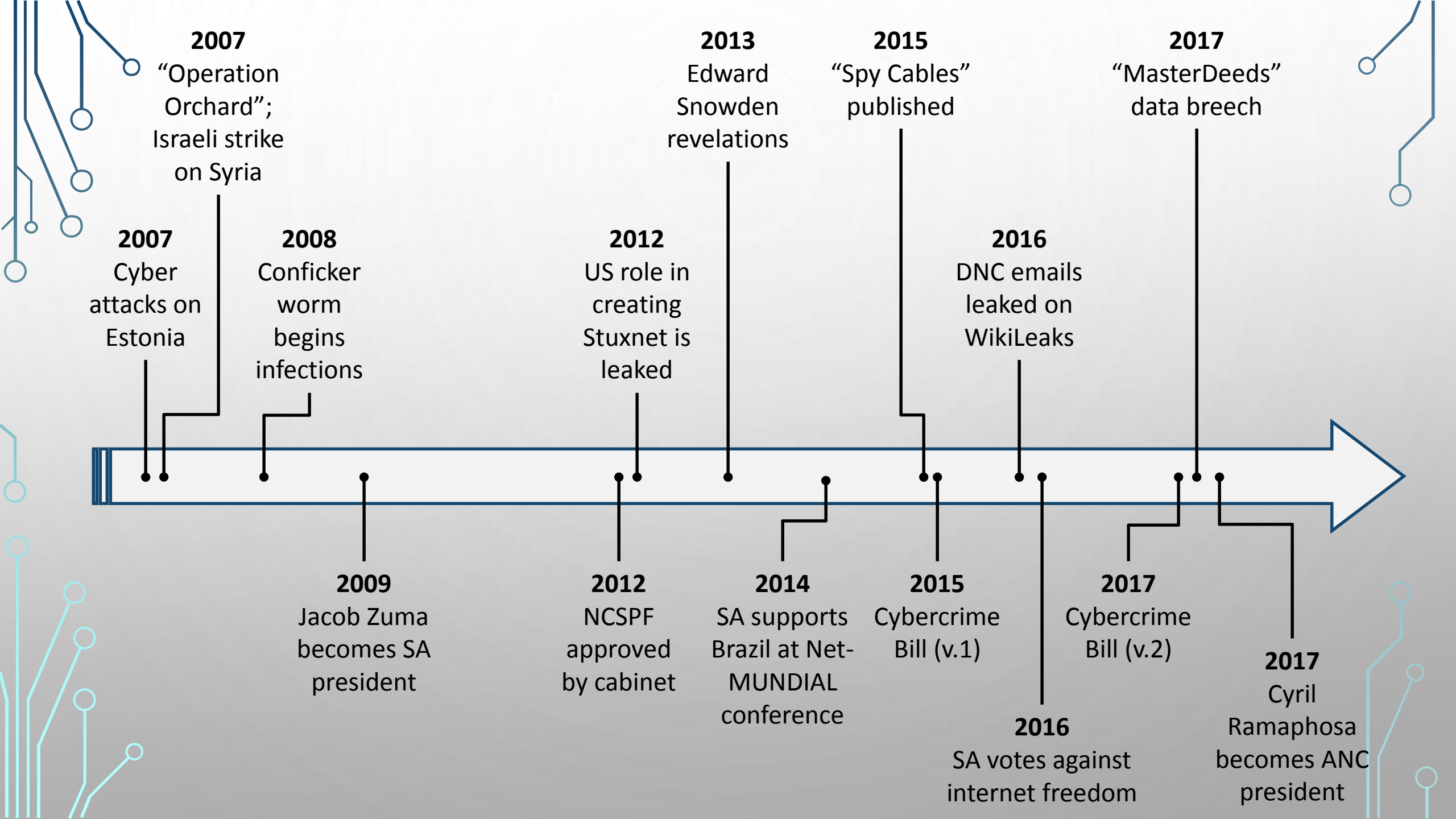


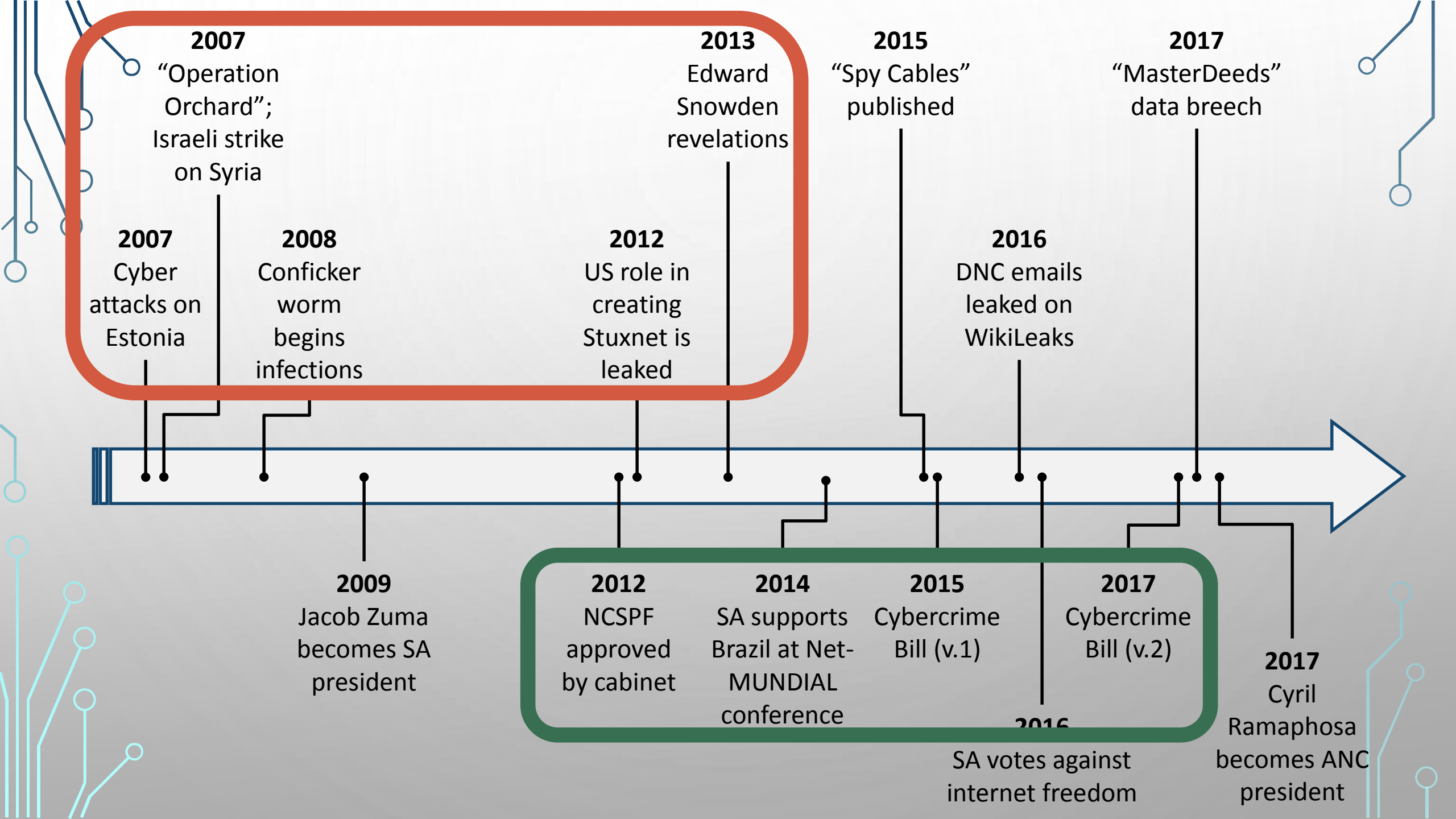
Jacob Zuma is
inaugurated as the
new president of
South Africa

1 APRIL, 2009: IRAN

The computer worm
Stuxnet is deployed
and begins to silently
penetrate the Iranian
nuclear programme







2007

"Operation Orchard";
Israeli strike
on Syria

2013

Edward
Snowden
revelations

2015

"Spy Cables"
published

2017

"MasterDeeds"
data breach

2007

Cyber
attacks on
Estonia

2008

Conficker
worm
begins
infections

2012

US role in
creating
Stuxnet is
leaked

2016

DNC emails
leaked on
WikiLeaks

2009

Jacob Zuma
becomes SA
president

2012

NCSPF
approved
by cabinet

2014

SA supports
Brazil at Net-
MUNDIAL
conference

2015

Cybercrime
Bill (v.1)

2017

Cybercrime
Bill (v.2)

2016



SA votes against
internet freedom

2017

Cyril
Ramaphosa
becomes ANC
president



WHAT I'D LIKE TO DO TODAY

1. Provide a framework for understanding the issue
 2. Describe South Africa's foreign policy in cyber space
 3. Explain why South Africa has made the choices it has
- 
- 

The image features a light gray background with a subtle gradient. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These elements consist of thin, dark blue lines in the top corners and teal lines in the bottom corners, with small circles at various points along the paths.

1. PROVIDING A FRAMEWORK



IN SOME RESPECTS, ALL STATES WANT TO ACHIEVE THE SAME THINGS...

1. Benefit from the economic potential of the internet
2. Spread their own political messages in cyberspace
3. Defend the integrity of their own networks
4. Collect intelligence on adversaries





HOWEVER, THERE ARE TWO IMPORTANT QUESTIONS THAT STATES NEED TO ANSWER

1. Is the open flow of information across the world beneficial to the national interest?
 2. Should the state prioritise the defence of its own networks, or its ability to attack the networks of other states?
- 
- 

LIBERAL VS. ILLIBERAL VIEWS ON THE FLOW OF INFORMATION

“OPEN INTERNET” VIEW

- Worries about cyber security as a technical problem
- Supports **multi-stakeholder** governance of the internet
- More prevalent in liberal democracies

“DIGITAL SOVEREIGNTY” VIEW

- Worries about subversive potential of “information warfare”
- Supports **multilateral** governance of the internet
- More prevalent in authoritarian states

PRIORITISING OFFENSE VS. DEFENSE

- The most effective exploits are “zero day” vulnerabilities
- After one is used, it is quickly patched
- Defence requires **cooperation** and **disclosure** to patch vulnerabilities
- Offence requires states to research and hoard vulnerabilities in **secret**



FOUR IDEAL TYPES OF FOREIGN POLICY IN CYBERSPACE

LIBERAL-OFFENSIVE

Open internet
Cyber attacks are a force multiplier
USA, Israel, Britain

LIBERAL-DEFENSIVE

Open internet
Cyber security through cooperation
Brazil, Estonia, Germany

ILLIBERAL-OFFENSIVE

Digital sovereignty
Cyber attacks are a balancing tool
China, Russia, Iran, North Korea

ILLIBERAL-DEFENSIVE

Digital sovereignty
Cyber security through self-help
Belarus

The slide features a light gray background with a subtle, large-scale pattern of concentric circles. In the four corners, there are decorative elements resembling circuit board traces or neural network connections. These elements consist of thin lines of varying colors (dark blue, light blue, and teal) that branch out and terminate in small circles.

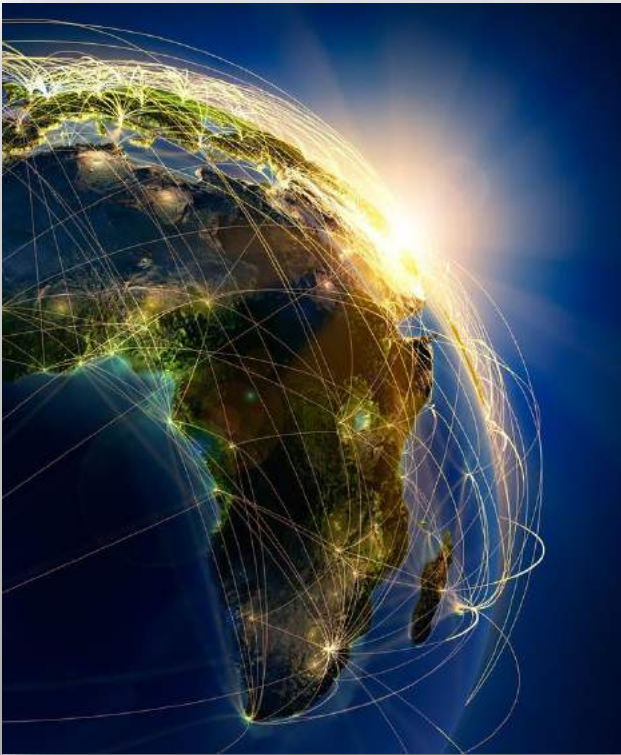
2. WHAT IS SOUTH AFRICA'S FOREIGN POLICY IN CYBER SPACE?

IS SOUTH AFRICA AN “OFFENSIVE” OR “DEFENSIVE” ACTOR?



- No evidence that SA has **ever** considered a cyber attack on another state
- Has not yet invested in offensive capability, even for deterrence
- Policies documents are focused on defence through self-help
- View cyber security mostly through the lens of crime & intelligence

IS SOUTH AFRICA A “LIBERAL” OR “ILLIBERAL” ACTOR?



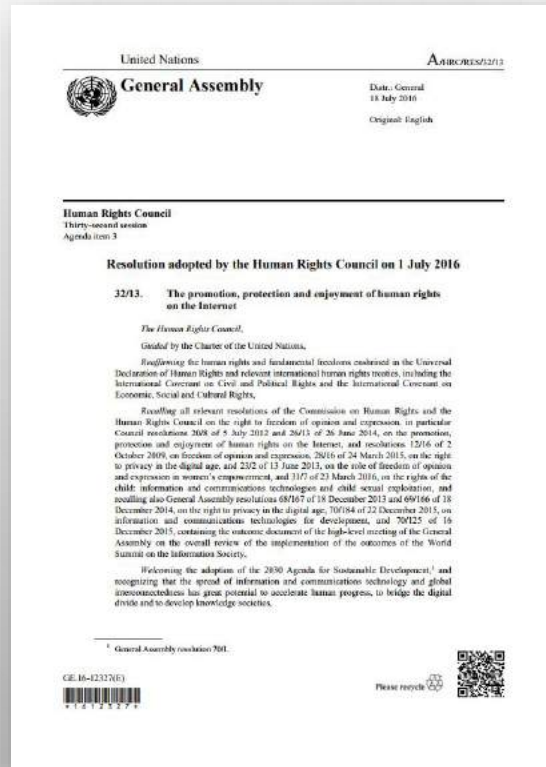
- South Africa's domestic policy:
 - Does not block social media apps
 - Does not restrict online political discussion
 - Does not arrest or punish people for online political speech
- Freedom House gives an internet freedom score of 25/100 (where 0 = completely free)

THIS IS (MOSTLY) REFLECTED IN SOUTH AFRICA'S FOREIGN POLICY

- Defines cyber security threats as attacks on networks, rather than “information warfare”
- Signed the 2001 Budapest Convention on cyber crime
- Supported the concept of multi-stakeholder at the NETmundial conference in Brazil in 2014
 - With Argentina, Brazil, France, Ghana, Germany, India, Indonesia, South Korea, Tunisia, Turkey, USA



THE GROWING ILLIBERAL TENDENCY IN SOUTH AFRICAN CYBER POLICY

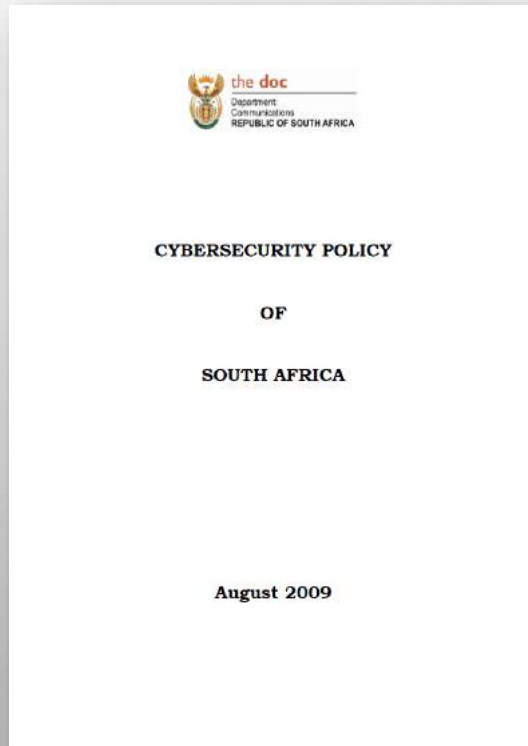


- The Film and Publications Amendment Bill introduced (2015) was seen as a creating an online censorship system
- Has never ratified the Budapest Convention
- Didn't sign the AU Convention on Cyber Security and Personal Data Protection (2014)
- Voted against online freedom at the UNHRC in 2016

The slide features a light gray background with a subtle, large-scale pattern of concentric circles. In the four corners, there are decorative elements resembling circuit board traces or neural network connections. These elements consist of thin lines of varying colors (dark blue, teal, and light blue) that branch out and terminate in small circles. The top-left and top-right corners have dark blue lines, while the bottom-left and bottom-right corners have teal and light blue lines.

3. EXPLAINING SOUTH AFRICA'S FOREIGN POLICY

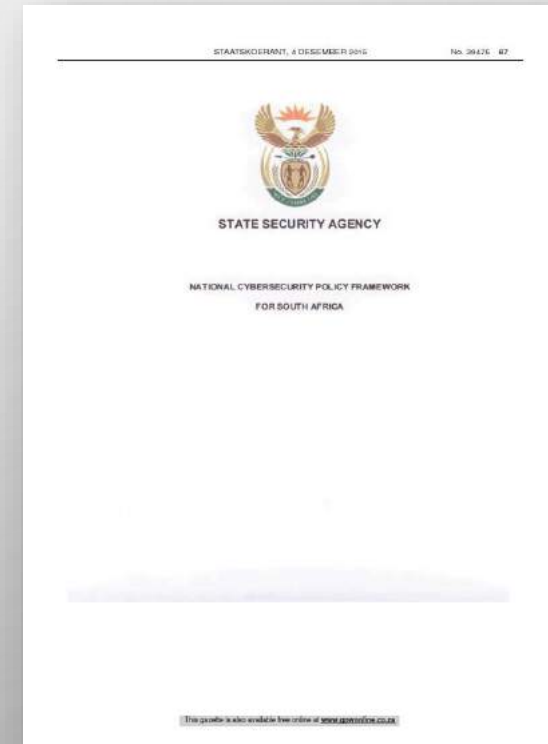
2009: DRAFT POLICY BY THE DEPARTMENT OF COMMUNICATIONS



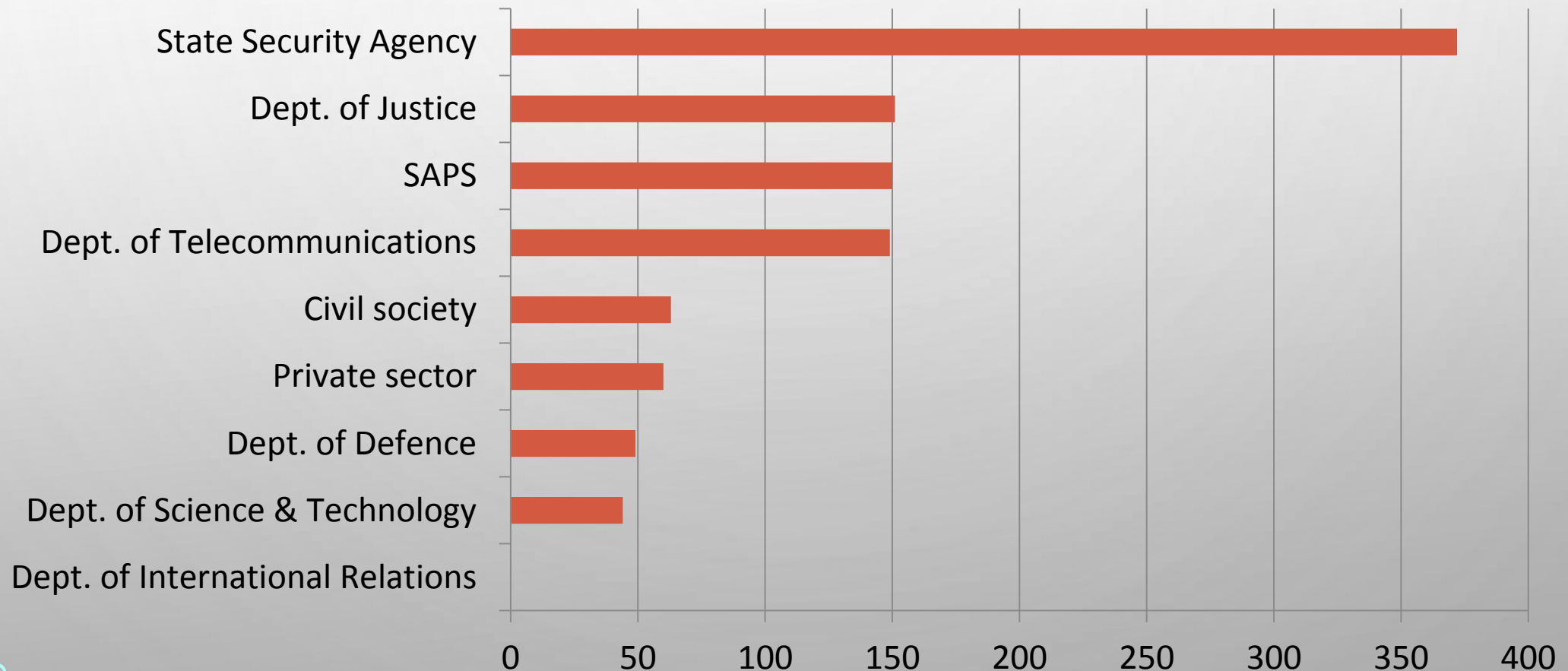
- This document gives us a sense of the Mbeki-era stance towards cyber security
- Focus is on co-operation:
 - Between South Africa and other states
 - Between state and non-state actors (civil society, business)
- Limited role given to intelligence or the military
- Leadership role given to Dept. of Communications

2012: NATIONAL CYBERSECURITY POLICY FRAMEWORK

- Calls for a two-track approach:
 - “Cyber Response Committee” (state security driven)
 - “Cybersecurity Hub” (civilian, public-private partnership)
- Citing the Russian cyber attacks on Estonia; views the problem as a **national security** threat
- Very limited focus on international co-operation
- Accords leadership role to the **State Security Agency**



HOW MUCH TEXT DOES THE N.C.P.F. DEVOTE TO EACH ACTOR?



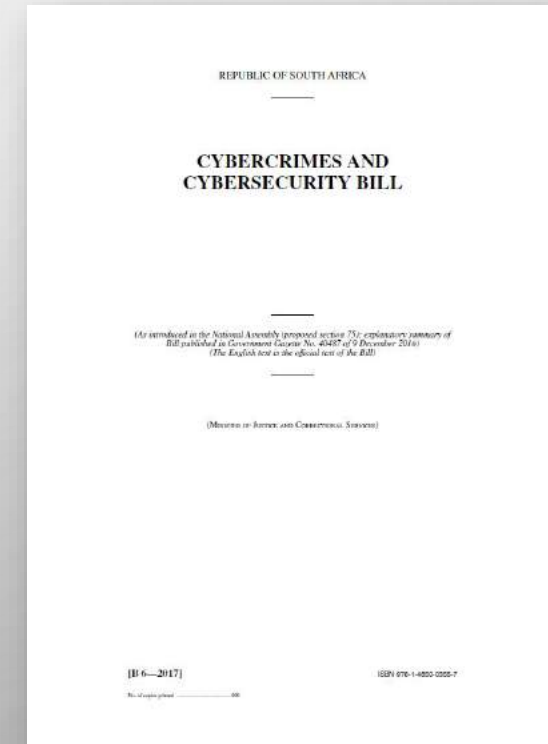
2012: RESEARCH ESSAY BY THE DEPARTMENT OF DEFENCE



- Evidence that the military was giving serious thought to the possibility of a cyber attack
- Heavy focus on national security and defence
- Sophisticated analysis of problems of attribution, deterrence, and *jus in bello*
- Implicitly considers whether SA should develop offensive capability (even if as a deterrent)

2015 & 2017: CYBERCRIME & CYBERSECURITY BILLS

- Once again, SSA is given a leadership role
- In addition, there are four other tracks:
 1. SSA to collect electronic signals intelligence
 2. SAPS to fight cyber crime
 3. Dept. of Telecommunications to co-ordinate with the private sector
 4. DoD to create a military Cyber Command





FAILURE OF THE CYBERCRIMES BILL

- The Cybercrimes Bill has been stuck in legislative hell for the past five years
- Bill in its current form is probably unconstitutional; will probably fail in judicial review
- Certain aspects of the Bill seem to have been written in order to advance the institutional interests of the intelligence community





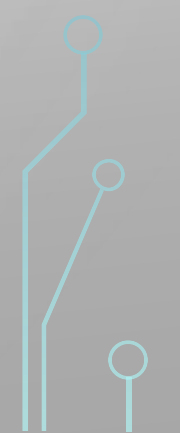

CONCLUSIONS: THE ROLE OF STRUCTURAL VARIABLES

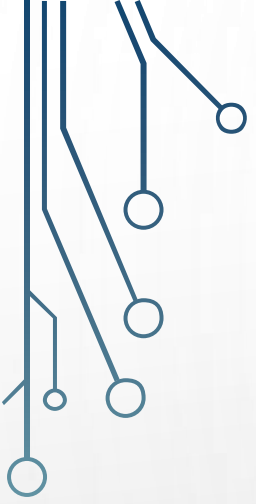
- During the Zuma Administration, the international system has provided clear signals that computers networks can be used to sabotage & subversion
 - However, there were several ways SA could have responded to this
 - Why did it choose a strategy focused on **defensive self-help** rather than co-operation (or attack)?
- 
- 



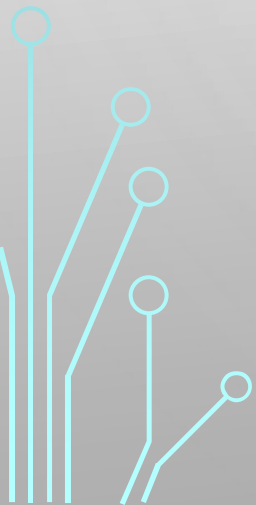
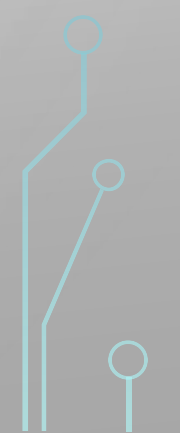
KEY VARIABLE:

The strategic culture of South Africa's
intelligence agencies







CONCLUSIONS: THE ROLE OF INTERVENING VARIABLES

- Institutional power over cyber security policy has clearly shifted from other agencies towards intelligence (SSA)
 - Part of broader trend towards “securitisation” under Zuma Administration
 - Informed by strategic culture of self-help, secrecy, and state-centrism
 - Will the change in ANC leadership usher in a new strategic culture?
- 
- 

USE OF CYBER POWER IN THE CONTEXT OF INTRA-A.N.C. POLITICS




#RamaphosaLeaks: Leaked Emails Revealed Cyril Ramaphosa's Love Affairs (wmescams.com)
promoted by tebogomolosi1



December 17, 2017 - Posted by admin in News and ANC, ANC elective conference, Breaking News, Cyril Ramaphosa, Dlamini-Zuma


Ramaphosa tries to collapse ANC elective conference in a Desperate move

Amidst the twists and turns going on in the ANC Elective Conference, reports are coming that the Cyril Ramaphosa (CR) faction is trying to collapse the 54th African National Congress...



Ramaphosa Bought Delegates Staying in Hotel Sponsored by Bidvest


Dec 17, 2017



#ANC54 – ANC Conference Day 1

Projections Show Competitive Edge

Dec 16, 2017



Dintle Schoeman · 2 days ago

This man has no stand in his life ... he is not only fake to country's people but also with his own wife ... Poor @RobyneClare .. incredible trustworthy person he is !! Round of Applase for him !!

^ | v · Reply · Share