Information Security for Researchers

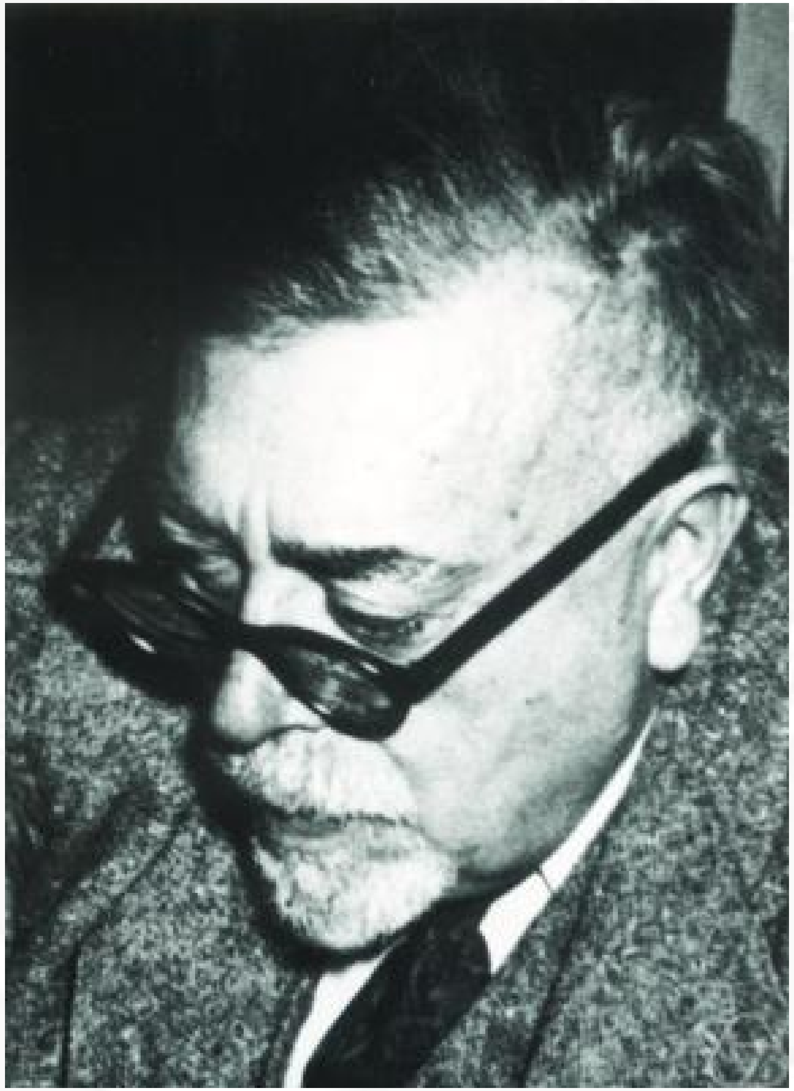
01/11/2018

Roshan Harneker
Jamiela Dawood

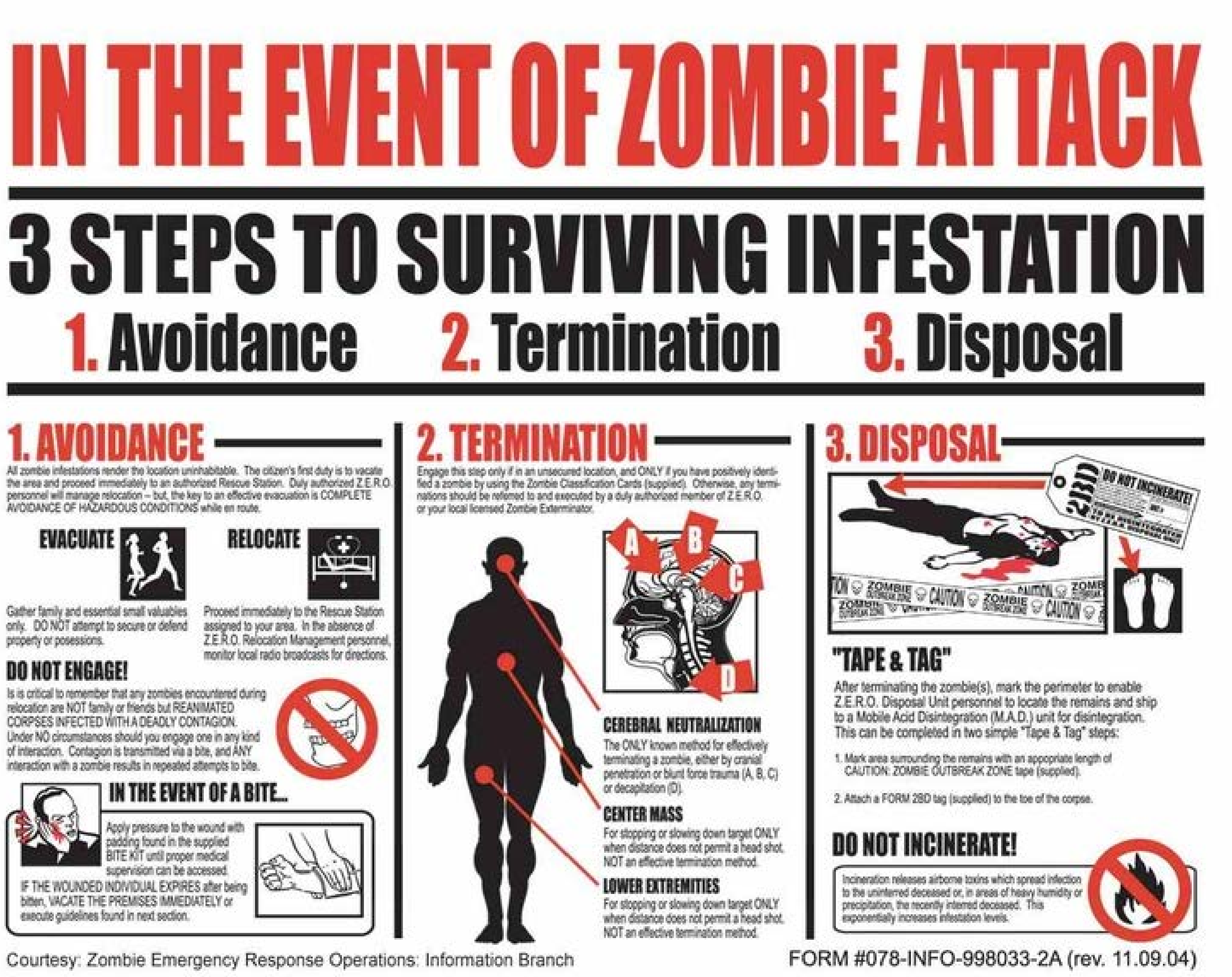
Norbert Weiner:
The Father of Cybernetics

“the physical functioning of the living individual and the operation of some of the newer communication machines are precisely parallel in their analogous attempts to control entropy through feedback.”

“What many of us fail to realize is that the last four hundred years are a highly special period in the history of the world. The pace at which changes during these years have taken place is unexampled in earlier history, as is the very nature of these changes. This is partly the results of increased communication, but also of an increased mastery over nature, which on a limited planet like the earth, may prove in the long run to be an increased slavery to nature. For the more we get out of the world the less we leave, and in the long run we shall have to pay our debts at a time that may be very inconvenient for our own survival.”



Source: Norbert Wiener (1950) *The Human Use of Human Beings: Cybernetics and Society*. revised in 1954.



IN THE EVENT OF ZOMBIE ATTACK

3 STEPS TO SURVIVING INFESTATION

1. Avoidance 2. Termination 3. Disposal

1. AVOIDANCE

All zombie infestations render the location uninhabitable. The citizen's first duty is to vacate the area and proceed immediately to an authorized Rescue Station. Duly authorized Z.E.R.O. personnel will manage relocation – but, the key to an effective evacuation is COMPLETE AVOIDANCE OF HAZARDOUS CONDITIONS while en route.

EVACUATE

Gather family and essential small valuables only. DO NOT attempt to secure or defend property or posessions.

RELOCATE

Proceed immediately to the Rescue Station assigned to your area. In the absence of Z.E.R.O. Relocation Management personnel, monitor local radio broadcasts for directions.

DO NOT ENGAGE!

Is is critical to remember that any zombies encountered during relocation are NOT family or friends but REANIMATED CORPSES INFECTED WITH A DEADLY CONTAGION. Under NO circumstances should you engage one in any kind of interaction. Contagion is transmitted via a bite, and ANY interaction with a zombie results in repeated attempts to bite.

IN THE EVENT OF A BITE...

Apply pressure to the wound with padding found in the supplied BITE KIT until proper medical supervision can be accessed.

IF THE WOUNDED INDIVIDUAL EXPIRES after being bitten, VACATE THE PREMISES IMMEDIATELY or execute guidelines found in next section.

2. TERMINATION

Engage this step only if in an unsecured location, and ONLY if you have positively identified a zombie by using the Zombie Classification Cards (supplied). Otherwise, any terminations should be referred to and executed by a duly authorized member of Z.E.R.O. or your local licensed Zombie Exterminator.

CEREBRAL NEUTRALIZATION

The ONLY known method for effectively terminating a zombie, either by cranial penetration or blunt force trauma (A, B, C) or decapitation (D).

CENTER MASS

For stopping or slowing down target ONLY when distance does not permit a head shot. NOT an effective termination method.

LOWER EXTREMITIES

For stopping or slowing down target ONLY when distance does not permit a head shot. NOT an effective termination method.

3. DISPOSAL

"TAPE & TAG"

After terminating the zombie(s), mark the perimeter to enable Z.E.R.O. Disposal Unit personnel to locate the remains and ship to a Mobile Acid Disintegration (M.A.D.) unit for disintegration. This can be completed in two simple "Tape & Tag" steps:

1. Mark area surrounding the remains with an appopriate length of CAUTION: ZOMBIE OUTBREAK ZONE tape (supplied).
2. Attach a FORM 2BD tag (supplied) to the toe of the corpse.

DO NOT INCINERATE!

Incineration releases airborne toxins which spread infection to the uninterred deceased or, in areas of heavy humidity or precipitation, the recently interred deceased. This exponentially increases infestation levels.

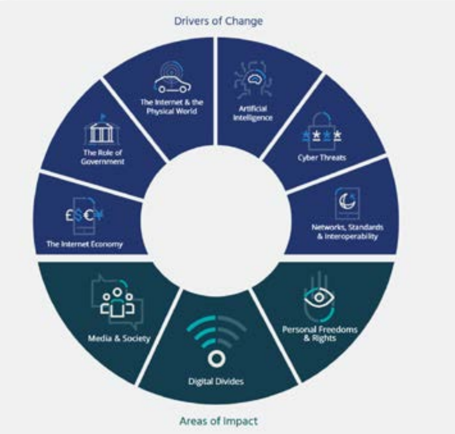
Courtesy: Zombie Emergency Response Operations: Information Branch

FORM #078-INFO-998033-2A (rev. 11.09.04)

Source: http://allthatsinteresting.com/survive-zombie-apocalypse/

How we see the Internet?

- Interoperability and mutual agreement
- Collaboration
- Tech as reusable building blocks
- No permanent favourites



2017

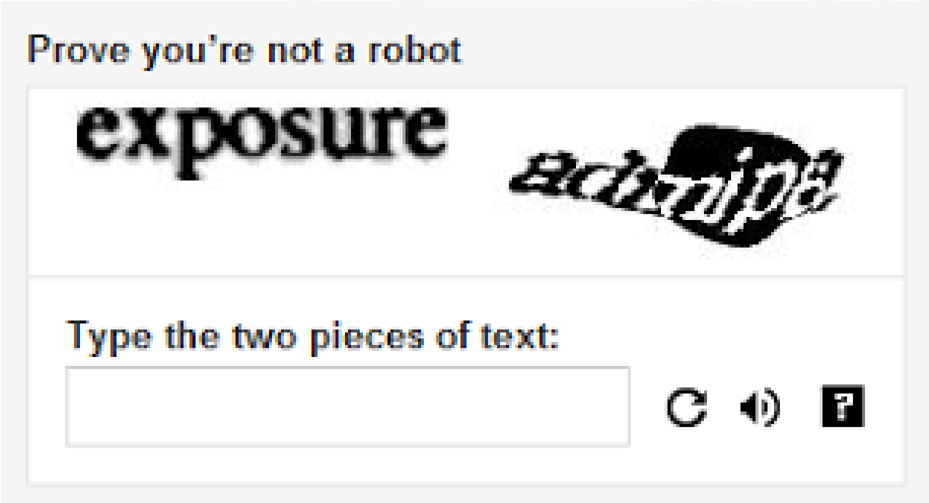
INTERNET SOCIETY GLOBAL INTERNET REPORT

Paths to Our Digital Future

Drivers of Change	Areas of Impact
The Internet Economy	Media & Society
The Role of Government	Digital divides
The Internet & the Physical World	Personal freedoms and rights
Artificial Intelligence	
Cyber Threats	
Networks, Standards & Interoperability	

Digitization of books

100 million words a day = 2 million books a year



Prove you're not a robot

exposure

Type the two pieces of text:

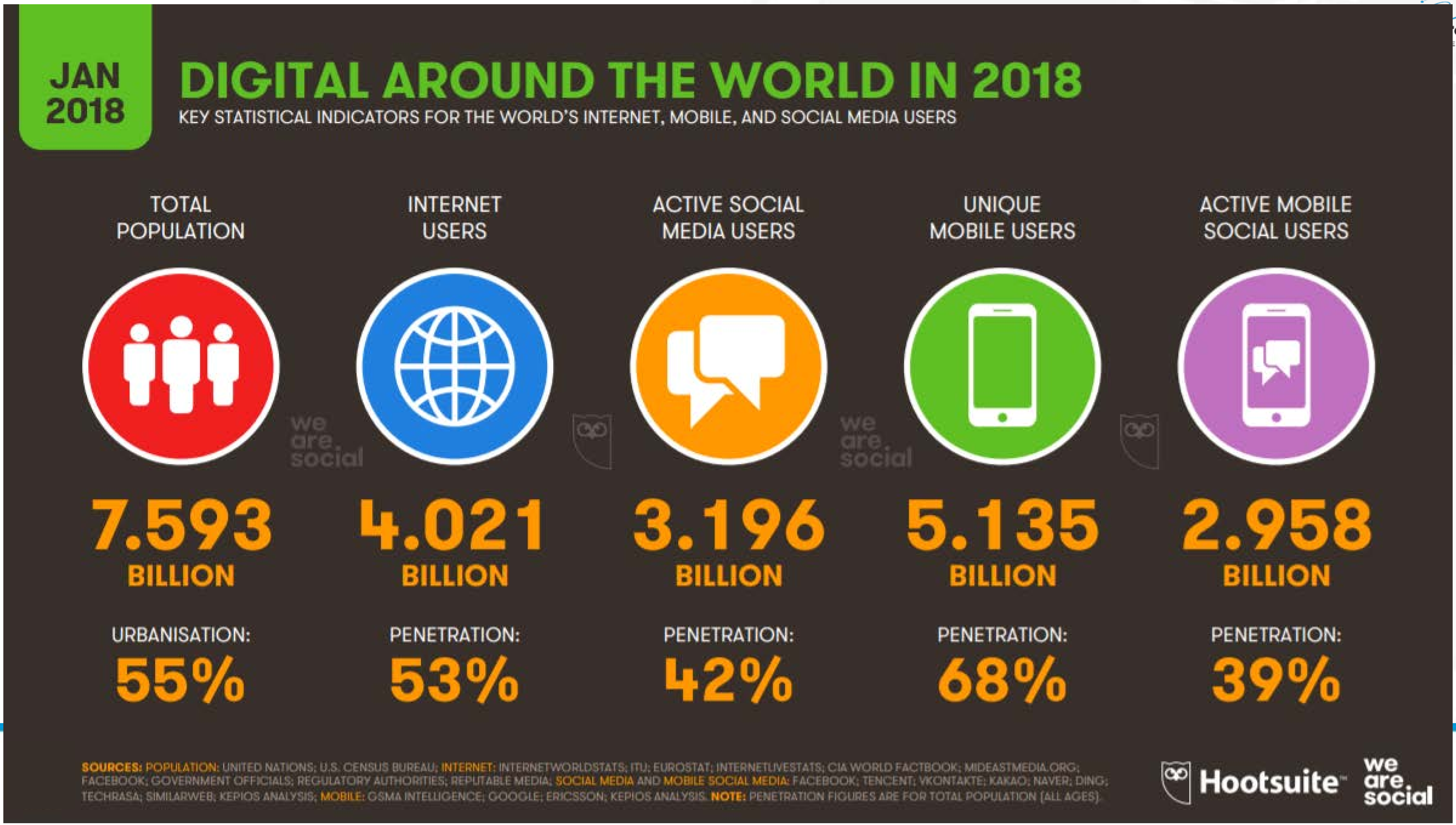
We possess the greatest capacity for good but also the greatest capacity for bad.

Top 5 most critical threats in 2018 :

- Phishing
- Ransomware
- Cloud security
- Data breaches
- Cryptocurrency mining

THREAT TOONS™
GUYS... IT'S TIME TO REINVENT YOURSELVES. KEYBOARDS ARE THE NEW KNIVES!
Old Villains Workshop

https://www.techrepublic.com/article/cybersecurity-rundown-the-5-most-critical-threats-to-businesses-in-2018/
https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/



JAN 2018

DIGITAL AROUND THE WORLD IN 2018

KEY STATISTICAL INDICATORS FOR THE WORLD'S INTERNET, MOBILE, AND SOCIAL MEDIA USERS

TOTAL POPULATION

7.593 BILLION

URBANISATION: 55%

INTERNET USERS

4.021 BILLION

PENETRATION: 53%

ACTIVE SOCIAL MEDIA USERS

3.196 BILLION

PENETRATION: 42%

UNIQUE MOBILE USERS

5.135 BILLION

PENETRATION: 68%

ACTIVE MOBILE SOCIAL USERS

2.958 BILLION

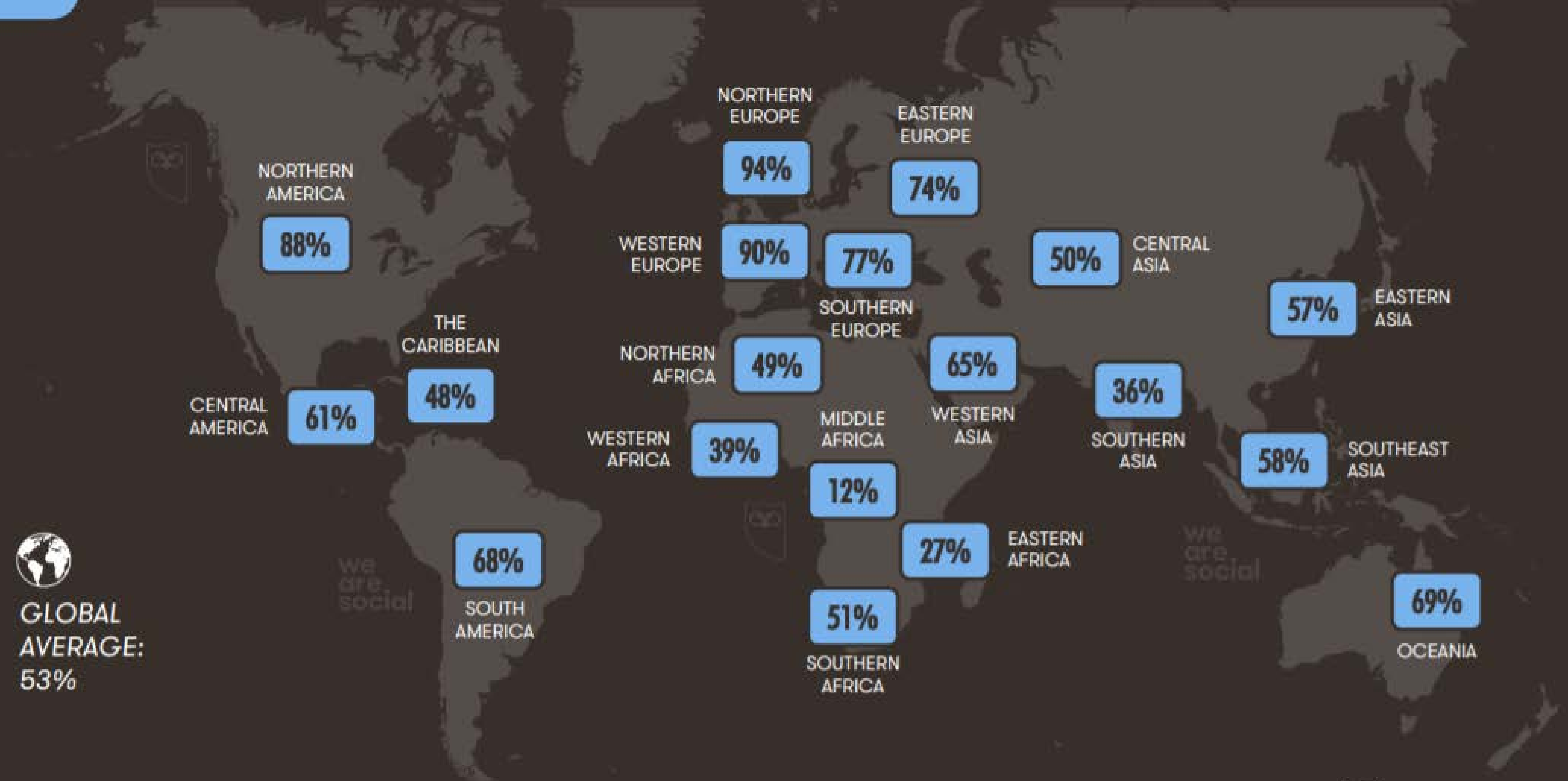
PENETRATION: 39%

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; **INTERNET:** INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; **SOCIAL MEDIA** AND **MOBILE SOCIAL MEDIA:** FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; **MOBILE:** GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. **NOTE:** PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).

JAN 2018

INTERNET PENETRATION BY REGION

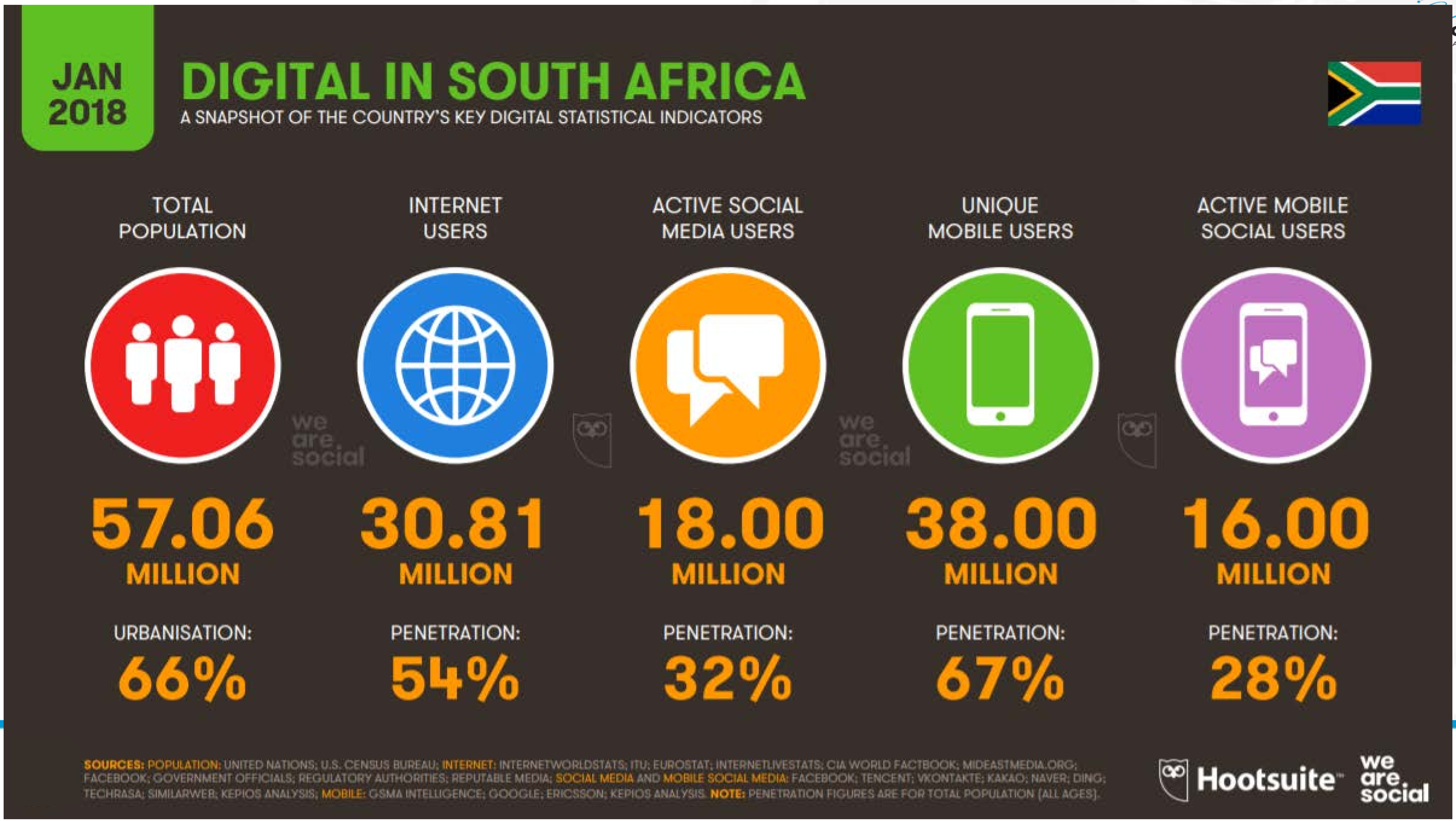
REGIONAL PENETRATION FIGURES, COMPARING INTERNET USERS TO TOTAL POPULATION



GLOBAL AVERAGE: 53%

SOURCES: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA. **NOTE:** PENETRATION FIGURES ARE FOR TOTAL POPULATION, REGARDLESS OF AGE.

Hootsuite we are social



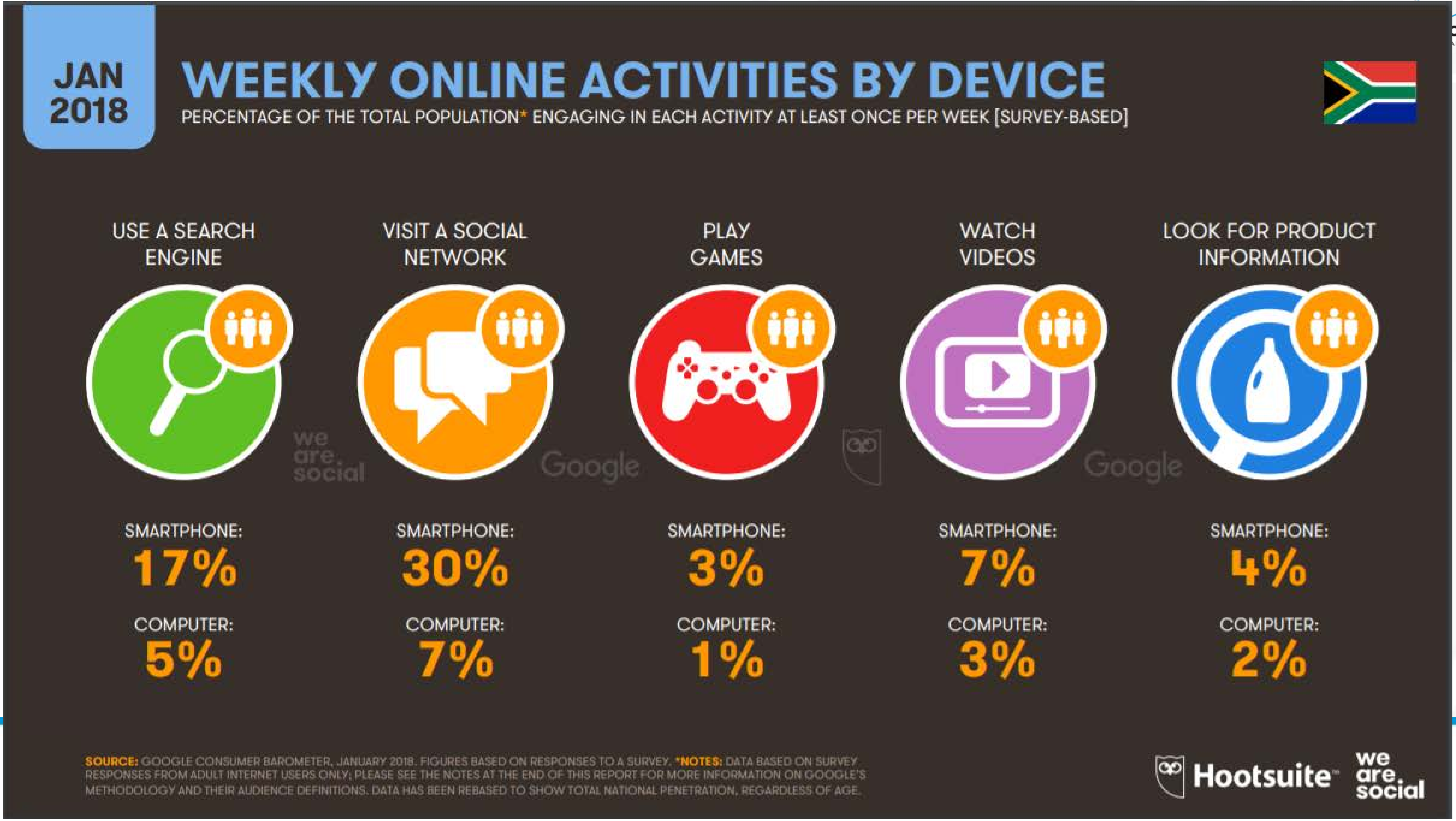
JAN 2018

DIGITAL IN SOUTH AFRICA

A SNAPSHOT OF THE COUNTRY'S KEY DIGITAL STATISTICAL INDICATORS

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
57.06 MILLION	30.81 MILLION	18.00 MILLION	38.00 MILLION	16.00 MILLION
URBANISATION: 66%	PENETRATION: 54%	PENETRATION: 32%	PENETRATION: 67%	PENETRATION: 28%

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; MOBILE: GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).



JAN 2018

WEEKLY ONLINE ACTIVITIES BY DEVICE

PERCENTAGE OF THE TOTAL POPULATION* ENGAGING IN EACH ACTIVITY AT LEAST ONCE PER WEEK [SURVEY-BASED]

USE A SEARCH ENGINE	VISIT A SOCIAL NETWORK	PLAY GAMES	WATCH VIDEOS	LOOK FOR PRODUCT INFORMATION
SMARTPHONE: 17%	SMARTPHONE: 30%	SMARTPHONE: 3%	SMARTPHONE: 7%	SMARTPHONE: 4%
COMPUTER: 5%	COMPUTER: 7%	COMPUTER: 1%	COMPUTER: 3%	COMPUTER: 2%

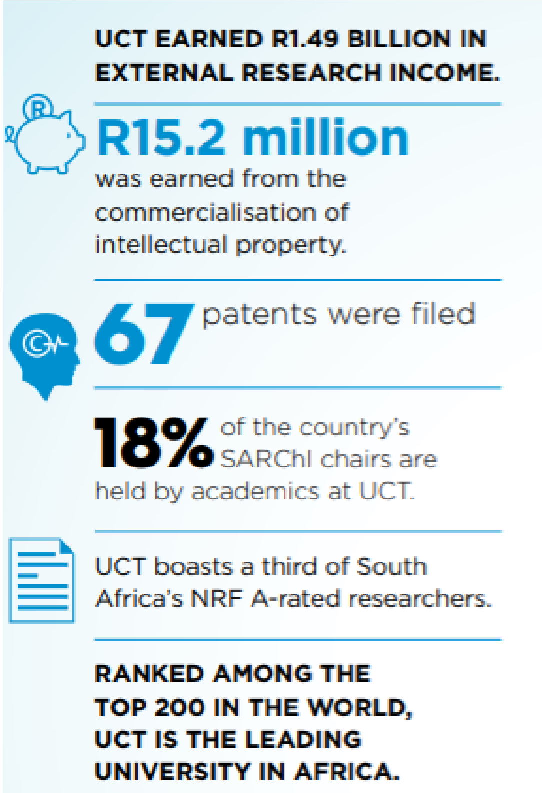
SOURCE: GOOGLE CONSUMER BAROMETER, JANUARY 2018. FIGURES BASED ON RESPONSES TO A SURVEY. *NOTES: DATA BASED ON SURVEY RESPONSES FROM ADULT INTERNET USERS ONLY; PLEASE SEE THE NOTES AT THE END OF THIS REPORT FOR MORE INFORMATION ON GOOGLE'S METHODOLOGY AND THEIR AUDIENCE DEFINITIONS. DATA HAS BEEN REBASED TO SHOW TOTAL NATIONAL PENETRATION, REGARDLESS OF AGE.

The UCT context?

Down the rabbit hole and into the fray....

28 185 students enrolled to study.

FEMALE
14 700
MALE
13 478



UCT EARNED R1.49 BILLION IN EXTERNAL RESEARCH INCOME.

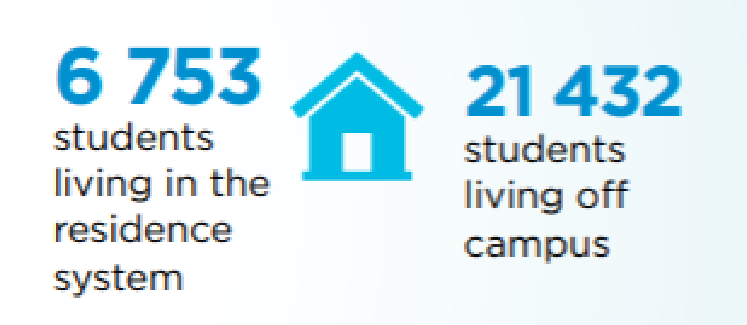
R15.2 million was earned from the commercialisation of intellectual property.

67 patents were filed

18% of the country's SARChI chairs are held by academics at UCT.

UCT boasts a third of South Africa's NRF A-rated researchers.

RANKED AMONG THE TOP 200 IN THE WORLD, UCT IS THE LEADING UNIVERSITY IN AFRICA.

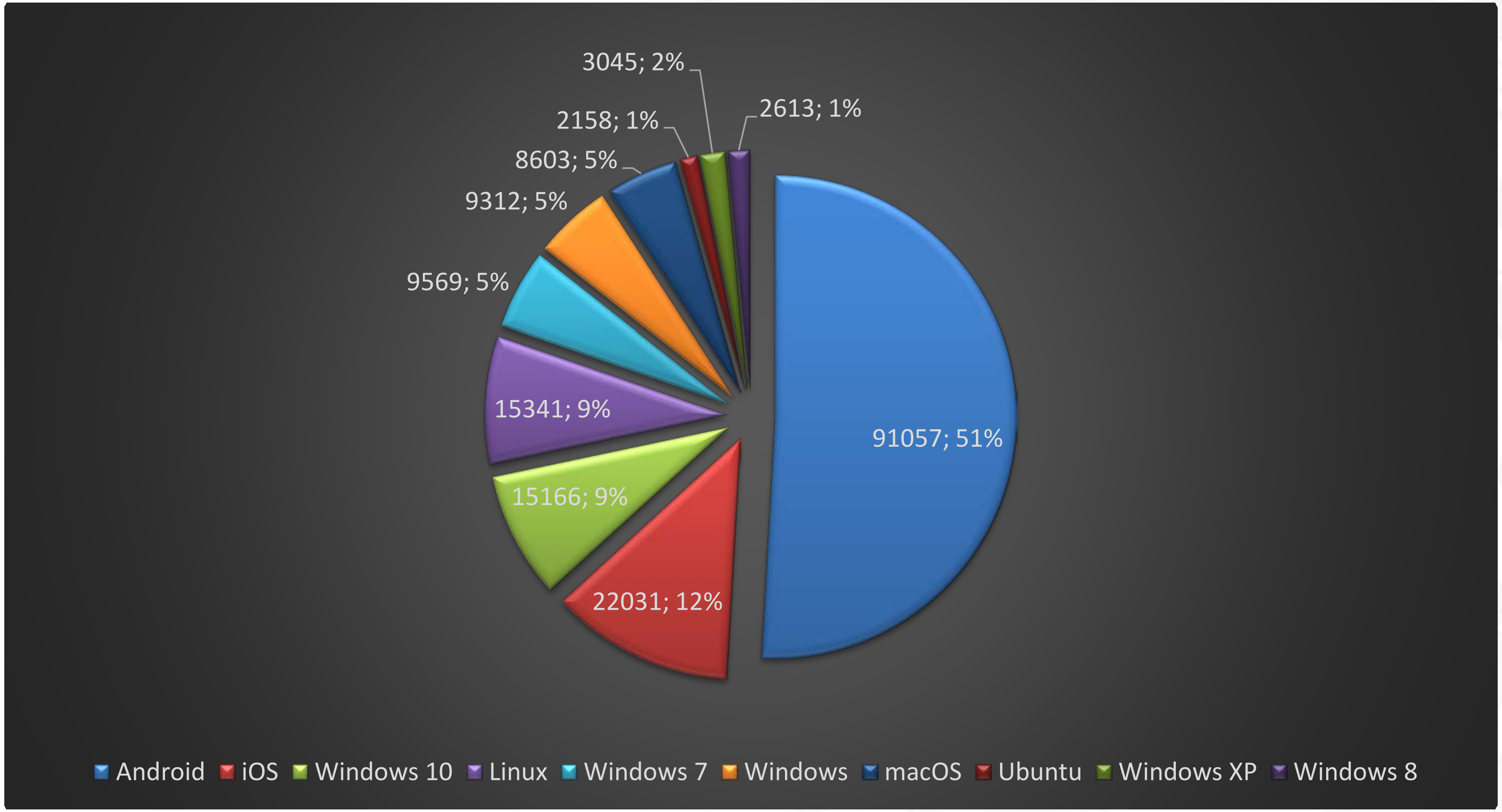


6 753 students living in the residence system

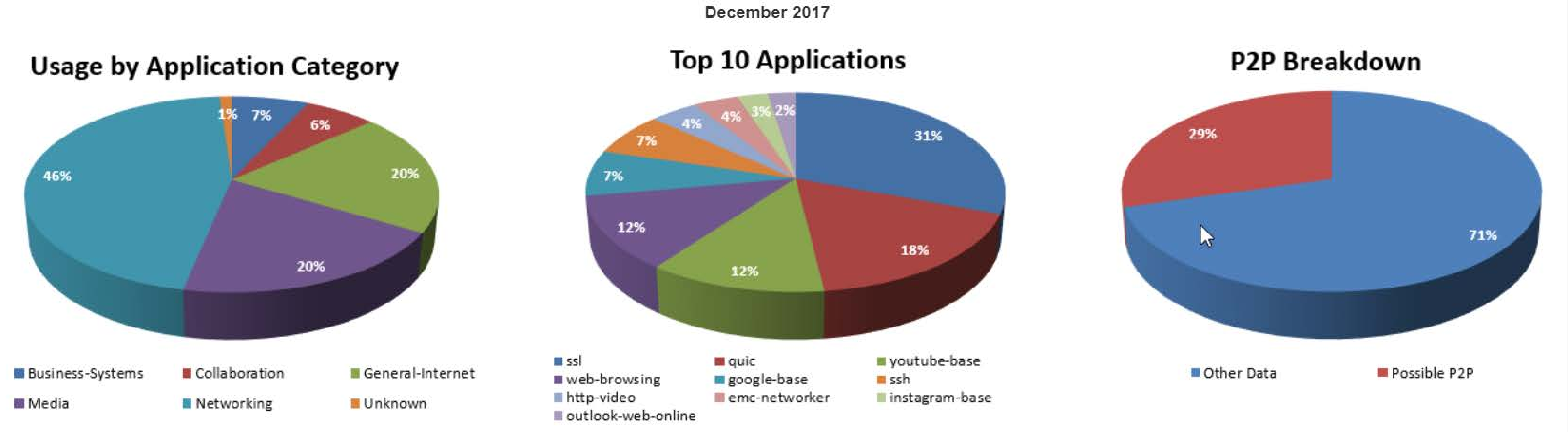
21 432 students living off campus

of 2017

Connected devices: 2017



Usage?



December 2017

Usage by Application Category

Top 10 Applications

P2P Breakdown

Who is responsible for security?

Everyone!

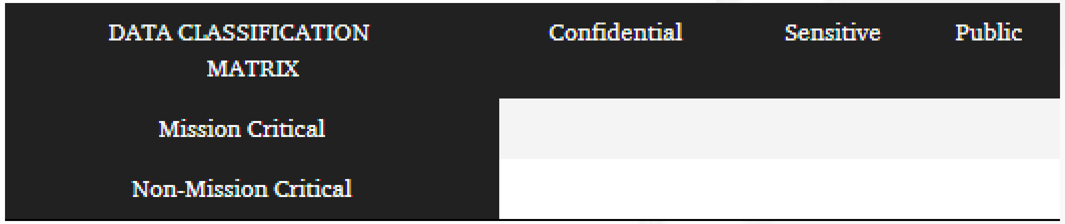
Protecting Your Research Data

- Passwords
- Outsmart the “phishing” attempt
- Check the sender address
- Antivirus
- Updates
- Mobile Device safety
- Social media safety
- Data classification
- System Authentication and Security
- Data encryption

Operating System Updates

- Update/patch OS regularly
- Windows OS
  - Enable automatic critical updates for Windows on a weekly basis
  - Enable WSUS updates
- Linux
  - Most *nix vendors release security patches regularly
  - check vendor websites for new patches
  - Subscribe to vendor mailing lists
- Use antimalware/antivirus apps

Data Classification



DATA CLASSIFICATION MATRIX	Confidential	Sensitive	Public
Mission Critical			
Non-Mission Critical			

- Data is classified to identify access control, data encryption and backup requirements.

System Authentication and Security

- ensure access to all confidential and sensitive data is managed appropriately
- use strong passwords
- change default “admin” accounts/passwords
- only allow connections from authorised users/ACLs
- conduct regular access reviews
- block access to ports not being used
- shutdown default services not being used
- blanket deny, then open access to ports required

System Authentication and Security

- enhance security of data by
  - restricting user access to directory file structure
  - restricting user permissions to directory file structure
- lock workstations when not in use
- use VPN for secure remote access to university computer systems

Data Encryption

- encryption may be used to further protect confidential and sensitive research data
- if data is encrypted, ensure that encryption is enabled for encryption in transit and at rest

Legal Considerations

Legal Considerations

- POPI compliance
- ECT Act
- PAIA
- GDPR

POPI

‘‘personal information’’ means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

UCT eResearch ACCELERATING RESEARCH

POPI

- record retention constraints
- data subject rights
- security safeguards
- notification of security compromise

Reporting cybersecurity threats

- Your web services and accounts have tools for reporting:
  - Harassment
  - Identity theft
  - Spam
  - Phishing
  - Inappropriate content, and more
- In South Africa, visit this site for a list of resources to report cybercrimes http://cybercrime.org.za/local-resources/
- At UCT, report all cybersecurity incidents to the CSIRT: csirt@uct.ac.za

Q&A

Thank you