20 August 2021

Cyber Intelligence Analysis

Critical insights into #FeesMustFall:
A cyber intelligence analysis

Snode

Table of contents

Introduction

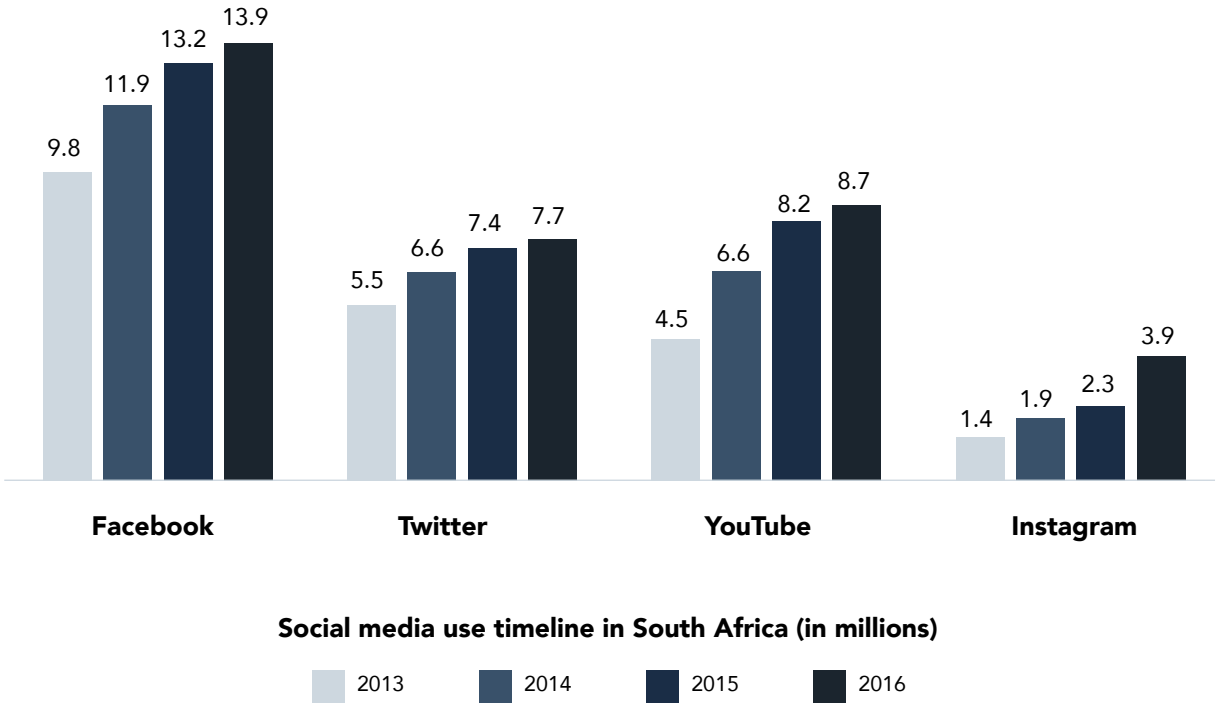
The student-led protest movement #FeesMustFall began in mid-October of 2015, galvanising learners and academics across the country to combat the increase in university fees and racial and gender inequalities on campus, while motivating for the decolonisation of the South African education system and increased government funding of tertiary studies.

The protests were peaceful in nature at first, as the consensus was clear that higher education was largely unaffordable for the majority of African students, but a sequence of events quickly drove the protests to violence (Ndelu, Edwin, Malabela, Vilakazi, Meth, Maringira, Gukurume & Kujeke, 2016). As the dissention gained in momentum, protestors used social media platforms such as Facebook, Twitter and Instagram to increase solidarity and mobilise other students in South Africa and around the globe through the hashtag #FeesMustFall (Dlamini, Malinga, Masiane, Maduvha Tshiololi, M, 2018).

This case study will investigate the role of social media advocacy in the protests, defined as an act of using digital technology to contact, inform, and mobilise a group of concerned people around an issue or cause (Kekana, Isaacs, Corke, 2015). Through this paradigm, this study will analyse the sources of online discourse and its role in escalating the violence during #FeesMustFall protests at the University of Witwatersrand, and how cyber intelligence can be used to predict - and potentially prevent - acts of violence.

The social media landscape in South Africa

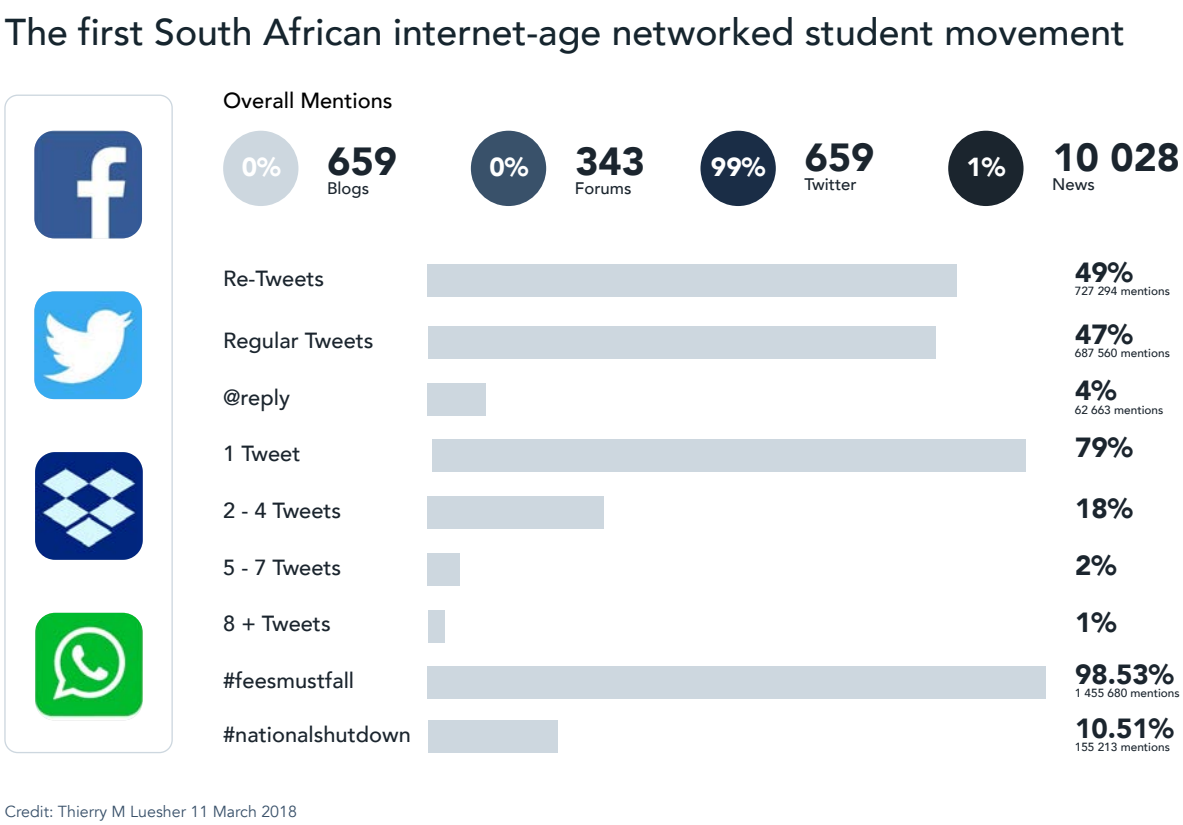
South Africa has an estimated 30.81 million internet users, meaning that almost 54% of the total population has access to the internet (Kemp, 2018). The most common internet application for South African adults is communication, followed by social networking and information seeking (McLeod, 2017).



Social media use timeline in South Africa (in millions)

Social media platforms have historically been used to stay in contact with friends and loved ones and document our lives online, however more than ever, social media is depended on as a valuable source of news (Nielson, Cornia, & Kalogeropoulos, 2016). While social media creates the opportunity to connect and communicate at an unprecedented rate, organisations and individuals with insidious motives may exploit these platforms for acts of terrorism and mass cognitive influence.

Analysing #FeesMustFall



Credit: Thierry M Luesher 11 March 2018

The dialogue around the movement was most prevalent on Twitter. Twitter as a platform is divisive by nature, but by delving deeper into the social sentiment around the movement and its sources, it became clear that outside influencers were making an impact on the #FeesMustFall narrative online. Numerous messages were exchanged under the guise of creating discourse around the cost of tertiary education.

Deciphering Twitter data

Snode's real-time data processing makes it possible to dissect a myriad of information contained within a tweet, including a Twitter user's real name, origin of the tweet (longitude and latitude), device type (iPhone or Android) and place of residence (e.g. city or hometown).
If users should share an image on Twitter, the metadata contained within that photo can offer a wide ranging array of insights, such as the location the photo was taken. Through the use of AI, it is possible to scan a digital image of someone and then discover their online profile.

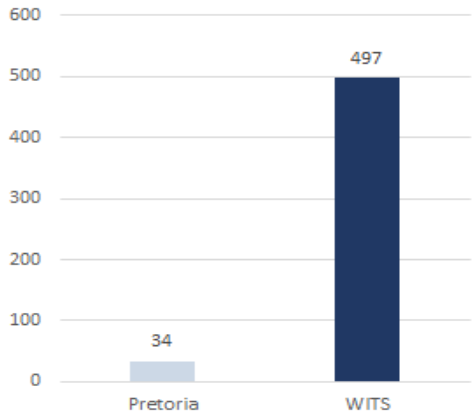
Through the use of AI, dynamic data and machine learning, Snode was able to fuse various social media conversations to identify emerging trends associated with, and patterns of behaviour fuelling this massive online campaign.

The sources of the underlying forces driving the #FeesMustFall protests online were surprising.

Discoveries

By analysing the anatomy of tweets, Snode discovered that many of the tweets did not originate from the same location that the message was referencing. In particular, the majority of tweets mentioning the University of Witwatersrand were found to have been sent from Pretoria, nearly 65 kilometres away.

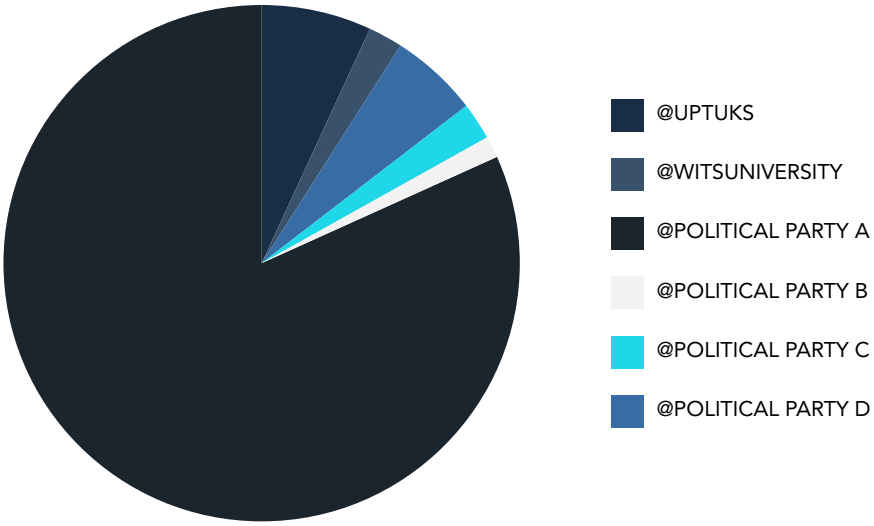
Using cyber intelligence to analyse the protes



Anomaly detection
Geo-location data

WITS was mentioned 497 times vs Pretoria's 34.
More source geo-locations were found in Pretoria.

In fact, Snode detected an anomaly in which tweets from South Africa's capital with the #FeesMustFall hashtag referenced Wits 14 times more than they did in their own city's university protest.



3%

Of #FeesMustFall tweets came from users linked to the @WitsUniversity handle

94%

Of #FeesMustFall tweets came from politically affiliated Twitter accounts

Accompanying this anomaly was the fact that only 3% of #FeesMustFall tweets came from users linked to the @WitsUniversity handle.

A staggering 94% of tweets came from politically affiliated Twitter accounts.

A political agenda

Based on these findings, it can be inferred that there was another agenda being played out, and the #FeesMustFall protests were being abused by some social media users to draw attention to other topics.

Snode's analysis of the #FeesMustFall movement identified the use of fake social profiles and significant political involvement, which influenced the movement, misrepresented the true aim of the students and skewed public perception of the nationwide riots.

More than a year after Snode's initial findings, the Inspector General of Intelligence (IGI) and the Independent Police Investigative Directorate (IPID) launched an investigation on whether a secret service agency was funding elements of the #FeesMustFall movement. Unnamed sources have alleged that crime intelligence agents recruited students to infiltrate and influence the protest action of the movement under the guise of a university bursary programme (Kekana, 2017).

Predicting outcomes through cyber intelligence

While disparate data creates uncertainty, it can be used to predict various high-risk events. Snode proactively responds to threats – by detecting imminent high-risk events before they happen - and identifying the golden thread between fake news and real-life results. The power lies in utilising mathematics to process disparate data, from multiple sources, in any format, at scale - all in real time.

Deep analysis of social media can also help those in positions of power make more informed decisions about what the public sentiment really is, and more importantly, from where it stems.

Defending the future

Easily accessible, open sources of cyber intelligence assist law enforcement and government services to predict and respond to critical events more efficiently. Cyber intelligence dynamic, real-time data could be used to predict natural disasters, disease outbreaks and threats to sovereign security or public safety. This includes combatting social evils such as human trafficking, organised crime, violent protest and acts of terrorism.

About Snode Technologies

Snode Technologies is a cyber defense company, operating out of Centurion, South Africa. Snode's defense model consists of people, processes, and expert technologies to provide superior real-time threat detection.

Snode's Guardian platform offers cyber threat intelligence empowering informed, data-driven, risk-based decision-making. It encompasses:

- Breach intelligence – insight into what attackers do once inside, how customer security controls fail
- Machine intelligence – with 80 global points of presence, thousands of malicious events per hour are collated
- Operational intelligence – experts validate alerts, and the continuous monitoring provides a unique perspective on identifying emerging global threats within specific industry verticals
- Adversary intelligence – intelligence analysts are entrenched within the mindset of an attacker and offer clients visibility into motives and trends

Our technology is next generation breach detection, offering real-time, contextual behavioural analytics to monitor and identify suspicious behaviour.

Author

Nithen Naidoo

CEO & Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerging Entrepreneur of 2021. Nithen is also a sought-after public speaker.

References

Dlamini, Z.I., Malinga, L., Masiane, T., Tshiololi, M. (2018). Social Media Advocacy in the #MustFall Campaigns in South Africa. Council for Scientific and Industrial Research, Pretoria, South Africa.

Kekana, M. (2017). Spy and Police Watchdogs Investigate Fees Must Fall Funding from Secret Service. Mail & Guardian. Retrieved from: https://mg.co.za/article/2017-10-31-spy-and-police-watch-dogs-investigate-feesmustfall-funding-from-secret-service/

Kekana, M., Isaacs, L., Corke, E. (2015). Tuition Fee Protests Shut Down 2 Of SA's Biggest Universities. Eyewitness News.

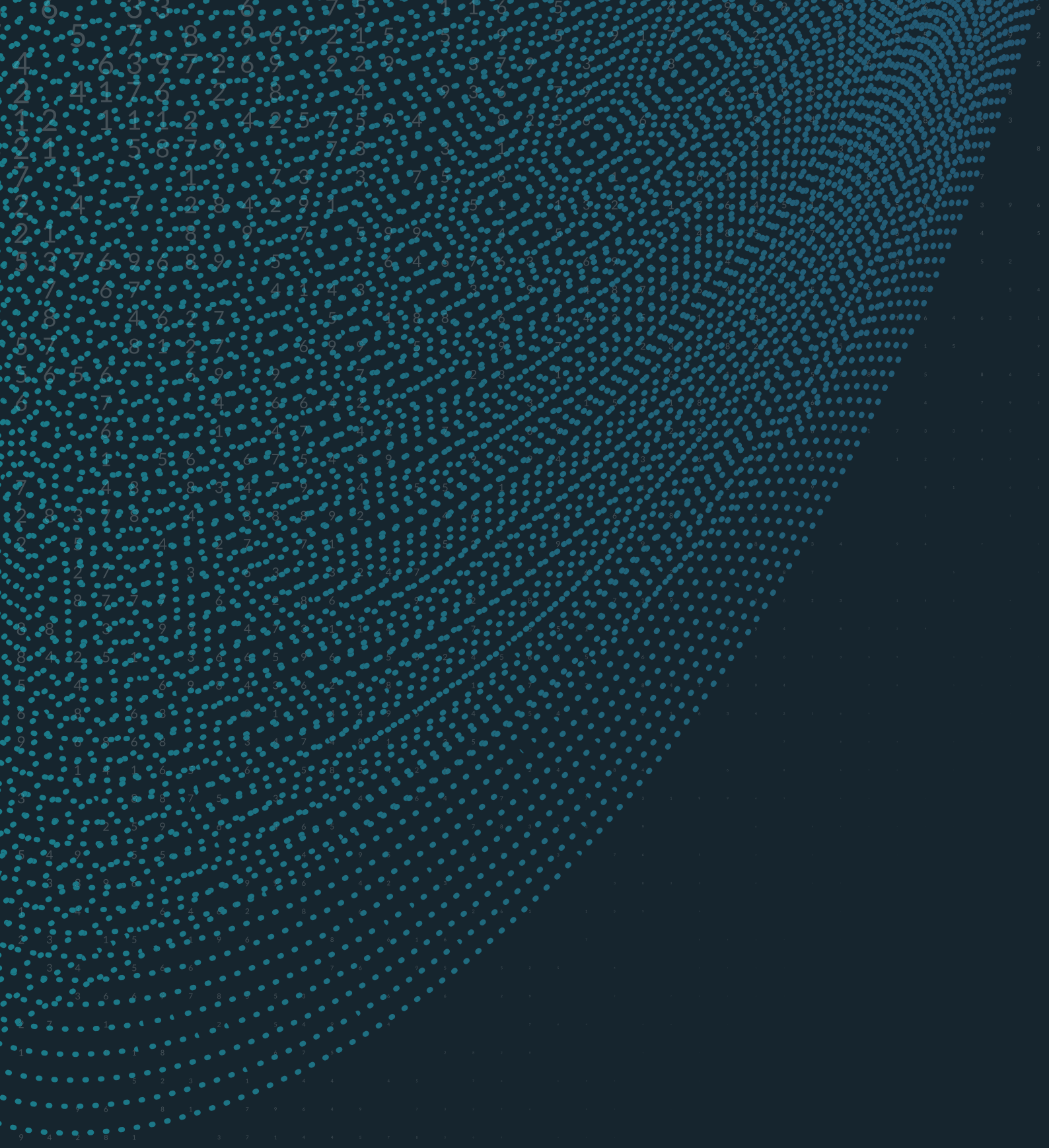
Kemp, S. (2018). Digital In 2018: World's Internet Users Pass The 4 Billion Mark. We are Social. Retrieved from:
https://wearesocial.com/blog/2018/01/global-digital-report-2018

Luesher, T.M. (2018) Internet Age Student Movement Research in the Era of Big Data and Social Media. Retrieved from: Internet-age student movement research in the era of big data and social media

McLeod, D. (2017). Internet Access In SA: Rural Areas Falling Far Behind. NewsCentralMedia. Retrieved from
https://techcentral.co.za/internet-access-sa-rural-areas-falling-far-behind/75789/

Ndelu, S., Edwin, Y., Malabela, M., Vilakazi, M., Meth, O., Maringira, G., Gukurume, S. & Kujeke, M. (2016). #Hashtag: An Analysis Of The Fees Must Fall Movement At South African Universities.

Nielsen, R. K., Cornia, A., & Kalogeropoulos, A. (2016). Challenges And Opportunities For News Media And Journalism In An Increasingly Digital, Mobile, And Social Media Environment. Council of Europe report DGI(2016)18. Reuters Institute for the Study of Journalism, University of Oxford.



Snode

www.snode.com
info@snode.com
+27 12 880 0989