https://doi.org/10.56273/1995-5928/2022/j19n2b1

Die evolusie van eietydse intelligensie en die rol van sosiale-media-intelligensie (Socmint)

Ansie Stegen en André Duvenhage

Ansie Stegen en André Duvenhage, Besigheidskool, Noordwes-Universiteit (Potchefstroomkampus)

Opsomming

Die afgelope aantal dekades is die internasionale sekerheidslandskap gekompliseer deur die snelle ontwikkeling van nuwe kommunikasietegnologie. Hierdie tegnologie hou nie net gevolge in vir die samelewing in die algemeen nie, maar ook vir politieke strukture en die intelligensie-gemeenskap in die besonder. Dit is veral die ontwikkeling van sosiale media binne die kommunikasie-omgewing wat ’n besondere uitdaging aan die intelligensiegemeenskap stel. Dit het ’n nuwe bron van inligting, naamlik sosiale-media-intelligensie (Socmint), tot gevolg gehad, met verreikende implikasies vir die spelreëls ten opsigte van intelligensie in al sy vorme en toepassings. Hierdie nuwe bron van inligting kan ’n belangrike rol in die intelligensieproses vertolk. Die ontwikkeling hou implikasies in vir intelligensiedienste wêreldwyd, maar ook vir die Suid-Afrikaanse intelligensie-omgewing wat met sy eiesoortige stel uitdagings te kampe het.

Trefwoorde: digitale era; grootdata; intelligensie; internet; kommunikasie; Socmint; sosiale media; Osint (inligting in die openbare domein); Sigint (inligting van onderskeppings)

Abstract

The evolution of contemporary intelligence and the role of social media intelligence (Socmint)

We are constantly being bombarded by the increasing pace of technological development. These developments affect every aspect of society, including business, education, communication and government. One of the most significant technological developments in recent decades, especially in relation to information communications, is the rise of the internet. This development has brought with it an information revolution that has increased the amount of available information, enhanced access to information and reduced the cost of communication.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Against this background, the main aim of this article is to explain the evolution of intelligence and the role of social media intelligence (Socmint). The article focuses on the following:

- The role and function of intelligence.
- The influence of technology in the development of intelligence.
- The post-Cold War period.
- Social media intelligence explained.
- Concluding remarks and perspectives.

The role and function of intelligence has remained the same throughout the ages: to identify threats to, and opportunities for national security. While the role and function has remained the same, the context in which the intelligence organisations function is dynamic and changes constantly. In order to remain relevant it is important for intelligence organisations to adapt to changing environments.

When the history of intelligence is examined, it is clear that the evolution of intelligence is closely linked to the development of technology. In this regard, World War I can be viewed as the beginning of the realisation of the importance and usefulness of intelligence. This can mainly be attributed to the technological developments towards the end of the 19th century, inter alia radiotelephony (developed towards the end of the 19th century), aviation and photography. The successful use of Sigint during World War I paved the way for its use during World War II, and played a crucial role in determining the outcome of the war.

Meanwhile, the end of the Cold War had a profound impact on intelligence organisations. Since then we have been living in a complex global environment where change is a given. One of the most significant developments associated with the internet is the emergence of social media, which changed traditional communication, augmented social interaction, and made state boundaries irrelevant. The phenomenon of social media plays a key role in the production and dissemination of information and people's access to it. Characteristics such as interactivity, affordability, availability, facelessness and a lack of censorship have increased the use of social media as a tool of communication. These same characteristics also make it attractive to terrorist and other criminal organisations. The implications for national security make social media important for intelligence organisations. Social media provide the intelligence community with a vast quantity of information (Socmint), that could be of importance in safeguarding national security. However, the intelligence community in South Africa is not using this tool to its full potential. This is evident from the July 2021 unrest. Just before and during this event people's social media were used to call the people to action. However, the intelligence community could not translate this information into actionable intelligence. This event can be classified as a huge intelligence failure. The community has not adapted to the new technological environment, rendering them irrelevant. It is time that the intelligence community in South Africa embraces technological change and includes Socmint as part of the gathering process. While Humint will remain an important part of the gathering process, the intelligence from social media can assist the intelligence community to stay relevant and be the preferred provider of intelligence.

Keywords: big data; communication; digital era; intelligence; internet; Osint; Sigint; social media; Socmint

https://doi.org/10.56273/1995-5928/2022/j19n2b1

1. Inleiding

Wêreldwyd het veranderende kommunikasietegnologie ’n integrale deel van ons daaglikse bestaan geword. Nuwe tegnologie verander lewenswyses en beïnvloed letterlik elke terrein van die groter samelewing. Tegnologiese verandering het ’n uitwerking op bykans elke aspek van ons lewens, byvoorbeeld besigheidsaktiwiteite, samelewingsinstellings, ekonomiese handelinge, finansiële bestuur en politieke besluitneming. Een van die grootste veranderlikes ten opsigte van die tegnologieveld was die ontwikkeling, vestiging en groei van die internet. Volgens DataReportal (2021) was daar teen Januarie 2021 reeds 4,66 miljard (ongeveer 59% van die wêreldbevolking) internetgebruikers in die wêreld, met 38,19 miljoen in Suid-Afrika. Die ontwikkeling het verdere stukrag gegee aan wat soms voorgehou word as die inligtings-revolusie. Een van die gevolge van hierdie kommunikasie-ontwikkeling is die verskynsel van sosiale media, wat ’n groot bydrae gelewer het tot die ontploffing van inligting in die openbare domein, of soos dit ook genoem word, grootdata (“big data”). In Januarie 2021 was daar oor die wêreld heen 4,2 miljard (ongeveer 53% van die wêreldbevolking) aktiewe gebruikers van sosiale media, met 25 miljoen in Suid-Afrika, volgens DataReportal (2021). Die inligting wat op sosiale media beskikbaar is, hou uiteraard bepaalde voordele en geleenthede vir die intelligensiegemeenskap in, maar skep ook probleme en stel uitdagings.

Intelligensiedienste is primêr gemoeid met die insameling van inligting om sake wat met nasionale sekerheid verband hou, te kan bestuur en hanteer. Die *inligtingsrevolusie* waarna hier bo verwys is, hou noodwendig verreikende implikasies in vir staatsveiligheidsagentskappe, oftewel intelligensiedienste wêreldwyd. Suid-Afrika is geen uitsondering op hierdie reël nie. Die geweld wat in Julie verlede jaar (2021) in KwaZulu-Natal (KZN) en dele van Gauteng uitgebreek het, waartydens skade van sowat R50 miljard aangerig is en meer as 300 mense gedood is, is onder andere gemobiliseer en aangehits deur van sosiale-media-platforms gebruik te maak (Hunter, Wicks en Singh 2021:11).

Teen hierdie agtergrond is die hoofdoel van hierdie navorsing daarop gerig om die invloed en impak van tegnologiese veranderings en vernuwing op die ontwikkeling van intelligensie-dienste te beskou, asook die noodsaaklikheid om by hierdie veranderende omstandighede aan te pas. Die studie is kwalitatief, deduktief en verkennend van aard en is gegrond op navorsing wat vir ’n PhD-studie aan die Noordwes-Universiteit gedoen is.[1] Die fokus van die ondersoek was veral gerig op Socmint (sosiale-media-intelligensie) en hoe dit die intelligensie-omgewings (met inbegrip van Suid-Afrika) kan en sal raak. Die fokus op Socmint as werkswyse en metodologiese benadering in die intelligensie-omgewing het in belangrikheid toegeneem sedert die beëindiging van die Koue Oorlog, nuwe tegnologiese ontwikkelings en veral inligtings- en kommunikasietegnologie. Laasgenoemde het saamgehang met wat algemeen as die “digitale revolusie” beskryf word. Wat gesien kan word as die inligtingsontploffing van die huidige tydsgewrig (en waarin sosiale media ’n uiters belangrike rol speel) het die wêreld en strategiese bedreigings verander en intelligensiedienste word gedwing om by veranderende omstandighede aan te pas en te vernuwe. Dit is ook die eis aan die Suid Afrikaanse intelligensie-omgewing en strukture wat hierdie taak moet vervul.

Die oogmerk van hierdie artikel is om die evolusie van eietydse intelligensie te omskryf, in die besonder die rol daarvan, asook om die plek van sosiale-media-intelligensie (Socmint) in dié verband uit te lig. Daar sal ook verwys word na die belangrikheid hiervan vir intelligensiedienste wêreldwyd en uiteraard ook in Suid-Afrika.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Fokuspunte van die navorsing sluit in:

- ’n Konseptualisering van *intelligensie*.
- Die doel en funksie van *intelligensie*.
- Die invloed van tegnologie op die ontwikkeling van intelligensiepraktyke.
- Die post-Koue Oorlog-era.
- Sosiale media en *Socmint*.
- Slotgedagtes en toepassingsperspektiewe.

2. Intelligensie: ’n konseptualisering en beskrywing

2.1 Gesaghebbende definiëring

Hoewel intelligensie, in die besonder spioenasie, al van Bybelse tye af teenwoordig is, is daar geen algemeen aanvaarde definisie vir die term nie. Die mees algemene definisie wat deur die meerderheid akademici en intelligensie-operateurs gebruik word, is dié van Kent (1966:ix): “the knowledge which our highly placed civilian and military men must have to safeguard the national welfare”. Verder verduidelik Kent (1966:ix) dat daar drie dimensies is waarna verwys word wanneer intelligensiewerkers (professionele intelligensiewerkers) die term *intelligensie* gebruik. Hierdie dimensies is die volgende:

- Intelligensie as ’n aktiwiteit (Kent 1966:ix): Die aktiwiteite word by die intelligensie-siklus ingesluit, en behels onder meer insameling, evaluering, ontleding, integrasie en verspreiding van inligting. Ons kan byvoorbeeld deur middel van intelligensie vasstel of ’n onwettige vergadering gaan plaasvind.
- Intelligensie as ’n produk (Kent 1966:ix): Die intelligensieproduk is die eindproduk van die intelligensieproses, byvoorbeeld: Intelligensie dui daarop dat ’n aanval op 23 September 2022 sal plaasvind.
- Intelligensie as ’n organisasie (Kent 1966:ix): Die intelligensie-organisasie is verant-woordelik vir die produksie van intelligensie, byvoorbeeld: Die minister het aan intelligensie die taak opgedra om die nodige inligting te verkry.

Hoewel daar nie ’n algemeen aanvaarde definisie vir intelligensie is nie, word Kent se definisie in die meeste gevalle as grondliggende vertrekpunt gebruik. Die verskillende definisies wissel van ’n deeglike en diepgaande beskrywing tot ’n meer saaklike beskrywing. Gill en Phythian (2006:1) beskryf intelligensie as:

> [...] an umbrella term referring to the range of activities (from targeting through the information gathering to analysis and dissemination) that are conducted in secret and aimed at maintaining or enhancing security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventative policy or strategy.

Hierdie definisie omskryf die volledige intelligensieproses. Warner (2002:15), daarenteen, omskryf intelligensie meer saaklik as: “secret state activity to understand or influence foreign entities”. Die staatsaktiwiteit waarna verwys word, sluit die intelligensiesiklus in, vanaf

https://doi.org/10.56273/1995-5928/2022/j19n2b1

insameling tot die verspreiding van die finale produk. Hoewel die meeste skrywers Kent (1966:ix) se definisie gebruik, is daar tog ander skrywers, soos Breakspear, wat ’n nuwe benadering tot intelligensie voorstel. Volgens hom (Breakspear 2013:692) is intelligensie: “A corporate capability to forecast change in time to do something about it. The capability involves foresight and insight, and is intended to identify impending change, which may be positive, representing opportunity, or negative, representing threat.” Hierdie definisie fokus op voorspelling en insig, wat in die huidige omgewing van snel veranderings en ontwikkelings baie belangrik is. Lowenthal (2020:1) fokus daarenteen meer op die kliënt en omskryf intelligensie as “information that meets the stated or understood needs of policy makers and has been collected, processed and narrowed to meet those needs. Intelligence is a subset of information. All intelligence is information, but not all information is intelligence.”

Binne die Suid-Afrikaanse konteks is die definisie, soos vervat in die Witskrif oor Intelligensie (1995), van toepassing. Volgens die Witskrif (Suid-Afrika 1995:2) is intelligensie:

> [T]he product resulting from the collection, evaluation, analysis, integration and interpretation of all available information, supportive of the policy and decision-making processes pertaining to the national goals of stability, security and development. Modern intelligence can be described as “organised policy related information, including secret information”.

Bogenoemde definisie ondervang sake soos:

- Die insameling van inligting wat betrekking het op bedreigings en geleenthede deur middel van alle beskikbare bronne.
- Die skryf van ’n produk deur die ontleding, integrasie en vertolking van beskikbare inligting (binne die intelligensie-omgewing bekend as *analise*).
- Tydige verspreiding van die finale produk na die kliënt (met betrekking tot die Departement van Staatsveiligheid is dit die President van Suid-Afrika, Minister in die Presidensie, asook ander staatsdepartemente).

Uit bogenoemde bespreking word intelligensie omskryf as (Stegen 2019:91):

- Die insameling van inligting wat betrekking het op bedreigings en geleenthede deur middel van alle beskikbare bronne (insluitend Socmint).
- Die skryf van ’n produk deur die ontleding, integrasie en vertolking van beskikbare inligting.
- Tydige verspreiding van die finale produk na die kliënt (met betrekking tot die Departement van Staatsveiligheid is dit die President van Suid-Afrika, Minister in die Presidensie, asook ander staatsdepartemente).

Die werksaamhede van die intelligensiegemeenskap vind binne die raamwerk van geheim-houding plaas en word bestuur deur prioriteite soos deur die kliënt (die regering van die dag) daargestel.

Uitgaande van bogenoemde konseptualisering en beskrywing word die doel en funksie van intelligensiedienste nou in meer besonderhede beskou.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

2.2 Doel en funksie van intelligensie

Die doel en funksie van intelligensie het deur die eeue heen dieselfde gebly. Volgens Lowenthal (2020:4) is die hoofdoel van intelligensie om die beleidsproses te ondersteun. Dit sal nietemin van pas wees om die omskrywing uit te brei en nasionale veiligheid in te sluit. Met bogenoemde in gedagte is die doel van intelligensie dus om die beleidsproses te ondersteun om sodoende nasionale veiligheid teweeg te bring.

In die Suid-Afrikaanse Witskrif oor Intelligensie (1995) word die doel van intelligensie soos volg beskryf:

- Om aan die beleidmaker tydige, kritiese en soms unieke inligting te verskaf, wat waarsku teen moontlike risiko's en gevare.
- Om geleenthede in die internasionale omgewing te identifiseer deur mededingers en hulle bedoelings en vermoëns te ontleed.
- Om goeie bestuurspraktyke te ondersteun deur kritiese intelligensie te verskaf, wat swakhede en foute uitwys.

Met die Witskrif as basis kan afgelei word dat een van die belangrikste funksies van 'n regering se intelligensiegemeenskap die beskerming en instandhouding van nasionale veiligheid is. Hierdie funksie is gekoppel aan die oogmerk van die regering om landsburgers te beskerm. Met betrekking tot die Suid-Afrikaanse konteks word die rol van die regering duidelik gestel in artikel 41 van die Grondwet (1996:22), waar aangedui word: "Alle regeringsfere en alle staatsorgane binne elke sfeer moet – (b) die welsyn van die mense van die Republiek verseker". Om hieraan te voldoen, voorsien die intelligensiegemeenskap die regering van tydige, unieke en akkurate inligting rakende bedreigings en geleenthede vir die Republiek. Hierdie inligting word benut om besluite te neem en beleid te formuleer of te hersien.

Om hierdie doel te verwesenlik het die intelligensie-organisasie drie funksies, naamlik waarsku, inlig en voorspel (Classen 2005:83). Die eerste funksie is om die regering te waarsku. Prioriteitsareas word bepaal en gemoniteer om verwikkelinge voortydig te identifiseer en die regering te waarsku. Dit bied die regering 'n geleentheid om beleidsveranderings of nuwe beleid te formuleer om sodoende nasionale veiligheid te beskerm. Die tweede funksie is om die regering in te lig oor nuwe neigings wat 'n uitwerking op nasionale veiligheid mag hê, hetsy negatief of positief. Die finale funksie is voorspellings oor moontlike bedreigings of geleenthede, sodat die regering kan optree. Dit stel die regering in staat om binne 'n vinnig veranderende omgewing aanpasbaar te wees.

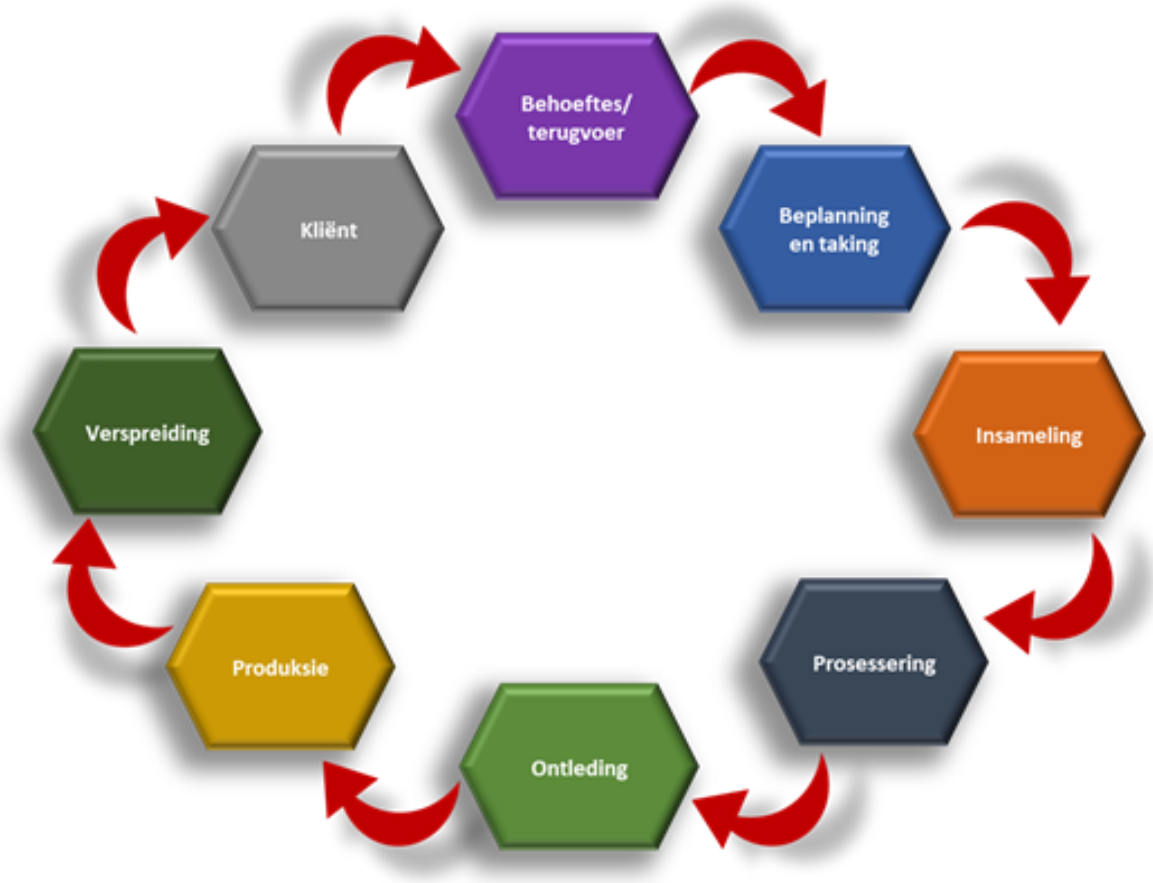
Om hierdie funksies te kan verrig, is dit ook belangrik om 'n begrip te hê van die intelligensie-proses en die elemente van intelligensie.

2.3 Intelligensieproses/-siklus

Die intelligensieproses bestaan uit bepaalde komponente (ook genoem aspekte of elemente) wat in wisselwerking met mekaar verkeer. Die elemente sluit sake in soos insameling, ontleding, teenspioenasie en koverte optrede. Hierdie elemente word saamgevoeg deur 'n model te skep om die volgorde te verduidelik van die aktiwiteite om inligting in te samel, te verwerk tot 'n produk en na die kliënt te versprei vir besluitneming, soos in figuur 1. Die elemente sluit in die

https://doi.org/10.56273/1995-5928/2022/j19n2b1

toeken van take (beplanning en taking), insameling en verwerking, ontleding en produksie, verspreiding aan, en terugvoer van die kliënt af (Johnson 2009:34; Lowenthal 2020:72–8).



Figuur 1. Intelligensiesiklus
Bron: Aangepas uit Lowenthal 2020:79

Dit is ook belangrik om die element te omskryf voordat die evolusie van intelligensie omskryf kan word, omdat die evolusie ook die elemente raak. Die eerste element is insameling. Volgens Lowenthal (2020:72) is insameling die hoeksteen van intelligensie, want daarsonder sou intelligensie bloot raaiwerk wees. Insameling word omskryf as die verkryging van inligting op verskeie maniere, soos gelei deur die regering se prioriteite en behoeftes (DCAF 2003:1, Lowenthal 2020:72). Die verskillende metodes van insameling sluit in:

- Humint (Human Intelligence): dit is inligting van menslike bronne verkry, ook bekend as spioenasie, waar persone gebruik word om inligting te bekom.
- Imint (Imagery Intelligence): intelligensie soos van foto's verkry.
- Sigint (Signals Intelligence), of Comint (Communications Intelligence): intelligensie verkry deur onderskepping van kommunikasiemiddele.
- Osint (Open Source Intelligence): inligting uit bronne wat in die openbaar beskikbaar is, soos joernale, tydskrifte, koerante en boeke.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Hoewel die verkryging van inligting deur menslike bronne (Humint) die oudste metode van insameling is, het tegnologiese ontwikkeling die hedendaagse bronne van inligting aansienlik uitgebrei. Om die funksies soos hier bo uiteengesit te vervul, is dit vir intelligensiedienste belangrik dat hulle organisasies met tegnologiese ontwikkeling moet byhou. Daarom was die hoofdoel van die studie waarop hierdie artikel gebaseer is, om die nuwe vorm van intelligensie, naamlik Socmint, in te sluit in die intelligensieraamwerk.

Die volgende intelligensie-element en volgende stap in die intelligensieproses is analise (prosessering, ontleding en produksie in bogenoemde siklus). Net soos geen inligting beskikbaar sou wees sonder insameling nie, sou daar ook geen intelligensie wees sonder ontleding nie. Analise is die proses waardeur inligting omskep word in intelligensieprodukte wat na die kliënt versprei word (Shulsky en Smitt 2002:41, Lowenthal 2020:76). Die doel van die analis is om die inligting tot intelligensie te omvorm deur inligting te kontekstualiseer en te vertolk, en om die implikasies vir nasionale veiligheid te beklemtoon. Die analis dryf die insamelingsproses deur behoeftes te identifiseer en te versprei, terugvoer te verskaf, en inligtingsgebreke aan die insamelingsafdelings oor te dra.

Die derde intelligensie-element is teenintelligensie, ook genoem teenspioenasie. Soos uit die bostaande figuur afgelei kan word, word hierdie element nie in die tradisionele intelligensie-siklus ingesluit nie. Dit vervul wel die belangrike funksie om die intelligensieproses teen vreemde intelligensiedienste te beskerm (Lowenthal 2020:201, Shulsky en Smitt 2002:99). Teenintelligensie is die optrede om buitelandse of vreemde intelligensie-insameling of -inmengingspogings, hetsy fisies, elektronies, in die kuberruimte of menslik, te identifiseer en te neutraliseer. Volgens ons is die staatskaping van die Zuma-era een van die grootste teenintelligensiemislukkings in die geskiedenis van Suid-Afrikaanse intelligensie. Die inmenging van buitelandse magte (die Guptas) moes vroeg reeds geneutraliseer gewees het. Die rede waarom dit nie gebeur het nie blyk duidelik uit getuienis voor die Zondo-kommissie, waar dit aan die lig gekom het dat die Departement van Staatsveiligheid ook gekaap was en dus nie hierdie taak kon vervul nie (Duncan 2017).

Die laaste element is koverte optrede, wat omskryf word as die geheime werksaamhede van een land om sy buitelandse beleidsdoelwitte te bereik deur die politieke, ekonomiese of militêre omstandighede in ’n ander land te beïnvloed (Lowenthal 2020:229, Shulsky en Smitt 2002:75). Koverte optrede is een van die mees omstrede funksies van die intelligensiebedryf. Dit is daaraan te wyte dat die geheime handelinge in ’n ander land uitgevoer word sonder die medewete van die spesifieke land waar dit uitgevoer word. Hierdie handelinge word as onwettig en inmenging in die soewereiniteit van die ander land beskou. In Suid-Afrika is koverte optrede onwettig en die intelligensiegemeenskap raak nie by sulke handelinge betrokke nie. Dit is nietemin algemene praktyk in die VSA. In 2013 het die CIA erken dat hulle betrokke was by die 1953-staatsgreep teen die Iranse Eerste Minister, Mohammad Mosaddegh (Lanz 2019).

Met hierdie bespreking van intelligensie as grondslag, fokus die volgende deel van die artikel op die rol wat tegnologie in die evolusie van intelligensie gespeel het.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

3. Die rol van tegnologie in die evolusie van intelligensie

Met die oog op hierdie artikel val die klem op die ontwikkeling van intelligensie sedert die Eerste Wêreldoorlog,[2] omdat dit die tydperk is waarin tegnologie ’n tersaaklike rol begin vertolk het.

Sowel die Eerste as die Tweede Wêreldoorlog het ’n belangrike bydrae gelewer om die belang van intelligensie na vore te bring. Die ontwikkeling van kommunikasietegnologie gedurende daardie tydperk het ’n waardevolle bydrae gelewer om die belangrikheid van intelligensie uit te lig.

Volgens Kahn (2006:84) het intelligensie nie ’n groot rol gespeel in die era voor die Eerste Wêreldoorlog nie, maar die situasie het redelik drasties verander tydens en na die genoemde oorlog. Die verandering in gesindheid teenoor intelligensie is hoofsaaklik te danke aan die ontwikkeling van kommunikasietegnologie soos die radio, telefoon, telegraaf en foto’s wat tydens die Eerste Wêreldoorlog bekendgestel is. Hoewel daar min inligting beskikbaar is oor tegnologie wat tydens die Eerste Wêreldoorlog gebruik is, kan dit tog beskou word as die keerpunt om die belangrikheid van tegnologie ten opsigte van intelligensie tydens oorlogspogings te beklemtoon.

Die insameling van inligting is een van die belangrikste elemente van intelligensie gedurende ’n spesifieke oorlog. Verskeie metodes van insameling word gebruik. Hierdie metodes sluit in: inligting van die soldate wat in gevegte betrokke was (inligting oor die vyand en gevegsmetodes), agente-netwerke (Humint) en onderskeppings (Sigint). Vanweë die beskadiging van landlyne as gevolg van oorloë, is eenhede in die verlede gedwing om radioverbindings en veldtelefone te gebruik. Hoewel dit kommunikasie vir die gevegseenhede vergemaklik het, het dit ook ’n geleentheid geskep vir onderskeppings (Sigint) deur die vyand. Hierdie situasie het aan intelligensiedienste die geleentheid gebied om tersaaklike, akkurate en tydige inligting aan eenhede te verskaf. Hoewel verskeie metodes van insameling tydens die Eerste Wêreldoorlog gebruik is, het Sigint ’n groot aandeel in die uitslag van dié oorlog gehad. Dit is waarom Ferris (1988:25) na die Eerste Wêreldoorlog verwys as die begin van moderne kommunikasie-intelligensie (Sigint).

Die suksesvolle gebruik van Sigint gedurende die Eerste Wêreldoorlog het die grondslag vir die gebruik daarvan in die Tweede Wêreldoorlog gelê. In die tydperk tussen die Eerste en die Tweede Wêreldoorlog het die Duitsers die Enigma-stelsel in gebruik geneem, wat ontwikkel is om diplomatieke en militêre kommunikasie te beskerm. In dieselfde tydperk kon die Pole daardie kommunikasie ontsyfer deur middel van ’n dekoderingsapparaat wat deur die Poolse wiskundiges Marian Rejewski, Jerzy Rozycki en Henryk Zygalski ontwikkel is (Baker 2018). Aan die begin van die Tweede Wêreldoorlog het die Pole hulle inligting oor dekodering aan die Britte verskaf. ’n Brit, Alan Turing, het Pole se aanvanklike ontsyfering verder ontwikkel. Dit het ook ’n belangrike rol in die uitkoms van dié oorlog gespeel. Sommige geskiedkundiges meen dat kriptografiese intelligensie die Tweede Wêreldoorlog met ongeveer twee jaar verkort het en ’n sentrale rol in die Geallieerde Magte se oorwinning gespeel het (Kahn 2006:132). Aangesien onderskeppingsintelligensie ’n beduidende rol tydens die Tweede Wêreldoorlog vervul het, is dit van pas om dié tydperk as die begin van die inligtingsoorlog te tipeer.

Die vroeë tot middel-20ste eeu het dus die grondslag vir die verhouding tussen tegnologie en intelligensie gelê. Hierdie verhouding is tydens die Koue Oorlog verder versterk. Die Koue

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Oorlog kan beskryf word as ’n intelligensie-oorlog tussen die Verenigde State van Amerika (VSA) en die Unie van Sosialistiese Sowjetrepublieke (USSR), toegespits op spioenasie, spesifiek met betrekking tot tegnologie. Albei lande het ’n verrassingsaanval deur die ander gevrees, daarom was die hoofdoel gedurende dié tydperk om geheime inligting in te samel deur Sigint, Imint en Humint te gebruik. Die internet en die persoonlike rekenaar was van die belangrikste tegnologiese ontwikkelings in dié tydperk. Volgens Hecht en Edwards (2010:288) het die rekenaar gedurende hierdie tydperk ’n belangrike rol in die ontwikkeling en produksie van kernwapens vervul. Die volle uitwerking van hierdie tegnologiese ontwikkelings is egter eers in die post-Koue Oorlog-era waargeneem. Ons is van mening dat sowel die USSR as die VSA meer staatgemaak het op die verkryging van inligting vanaf menslike bronne (Humint). Dit blyk uit die aantal spioene wat gedurende hierdie tydperk gevange geneem is. Inligting met betrekking tot Sigint in hierdie era is moeilik bekombaar as gevolg van die geheimhouding rondom die kwessie.

In die tydperk wat ná die Koue Oorlog gevolg het, het twee belangrike gebeure ’n impak op intelligensiegemeenskappe gehad. Die eerste was die einde van die Koue Oorlog. Intelligensie-dienste was tydens die Koue Oorlog deeglik bewus van hulle vernaamste doelwitte en fokusareas. Dit het egter verander met die val van die Berlynse muur, waarna die vyand nie meer so duidelik gedefinieer was nie.

Die tweede gebeurtenis was die ontwikkeling en groei van die inligtings- en kommunikasie-tegnologie (IKT). Die internet is gedurende die Koue Oorlog ontwikkel, waarna verdere ontwikkeling daarvan gedurende die post-Koue Oorlog-era die demokratisering van inligting teweeggebring het. Die internet het toegang tot inligting verhoog, die koste van kommunikasie verlaag, en ’n inligtingsontploffing (grootdata) tot gevolg gehad. Volgens Vaisman en Zimanyi (2014:507) is grootdata ’n groot versameling data wat ongestruktureerd is en teen so ’n vinnige koers groei dat tradisionele dataverwerkingstelsels dit nie kan bestuur of ontleed nie. Gartner (2016) verduidelik dat grootdata drie hoofeienskappe het, naamlik ’n groot hoeveelheid data (“volume”), ’n wye verskeidenheid datatipes (“variety”) en hoë snelheid (“velocity”). In hierdie verband lewer sosiale media ’n groot bydrae tot grootdata (Matilda 2016:2).

Sekere eienskappe van die internet het die grondslag gelê vir die ontwikkeling en groei van sosiale media. Die eerste van hierdie eienskappe is die globale aard van die internet (Internet Society 2016:2). Volgens Statistica (2021) was daar in Januarie 2021 net vier lande met ’n internetpenetrasie van minder as 10% (Noord-Korea, Eritrea, Suid-Soedan en die Comore). Hierdie globale aard van die internet speel ’n groot rol in die sosiale media, waar inligting teen ’n vinnige tempo gelyktydig na ’n groot groep mense versprei kan word. ’n Volgende belangrike eienskap is die interaktiwiteit van die kommunikasie, sonder inagneming van grense (Potts 2014:7). Inligting kan oor landsgrense heen versprei word sonder om gehoor te gee aan regulasies en wetgewing in ander lande. Dit is ook maklik toeganklik (Potts 2014:5). Die koste van konnektiwiteit is laag en enige persoon met ’n selfoon of rekenaar en internettoegang kan inligting skep en versprei. Die internet bied ook die geleentheid tot anonimiteit (Potts 2014:7). Inligting kan versprei word en kommentaar kan gelewer word sonder om jou identiteit bekend te maak. Teen hierdie agtergrond is dit dus gepas om na hierdie tydperk as die sosiale-media-era te verwys.

Voordat sosiale media en Socmint bespreek kan word, is dit noodsaaklik om die post-Koue Oorlog-era waarbinne die intelligensiegemeenskap funksioneer te verduidelik, waar tegnologie tot ’n groot mate die nuwe werklikheid geskep het en steeds skep.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

4. Post-Koue Oorlog-era

In die post-Koue Oorlog-era verander die wêreld daagliks en teen ’n toenemend vinniger pas. Dit impliseer dat alle regeringsdepartemente by die omstandighede moet aanpas, net soos die intelligensiedienste. Dit is hierdie organisasies wat veral deur die veranderde omgewing geraak word met betrekking tot die fokus, uitvoering van pligte, manier van funksionering en mandaat. Volgens Rathmell (2002:87) het die einde van die Koue Oorlog, asook die inligtingsrevolusie, bronne en wyses van funksionering binne die intelligensiegemeenskap beïnvloed, daarom is dit uiters noodsaaklik om hierdie nuwe werklikheid te vertolk en te bestuur. Wanneer Rathmell se verduideliking van die nuwe omgewing ondersoek word, kan tegnologie asook sosiale media duidelik waargeneem word.

Hy verwys eerstens na die einde van metanarratief (Rathmell 2002:95). Dit is vervang deur ’n gefragmenteerde wêreldsiening, waarbinne daar geen eenvormige teorieë oor die sosiale wêreld of oor kennis op sigself is nie. Binne hierdie nuwe omgewing moet die intelligensiegemeenskap nuwe bedreigings identifiseer en ’n nuwe rol vind. ’n Deel van die nuwe bedreigings is dié wat met sosiale media gepaardgaan en later in die artikel bespreek word.

’n Volgende kenmerk van hierdie nuwe omgewing waarin ons werk is die afwesigheid van sentrums, gepaardgaande met onsekere identiteite, waar sosiale veranderings, tegnologie en ekonomiese vooruitgang individuele identiteitsgrense afbreek, en individue sonder ’n identiteit skep (Rathmell 2002:95). Die beëindiging van die Koue Oorlog asook die inligtingsrevolusie het die situasie verander en daar is geen sekerheid meer oor wie die vyand of kliënt is nie. ’n Ander kenmerk wat baie nou aansluit by die vorige, is vloeibare grense waar sosiale veranderings, tegnologie en ekonomiese vooruitgang versteurde grense tussen state, streke en maatskappye veroorsaak en ’n omgewing meebring waar die soewereiniteit van state geïgnoreer word (Rathmell 2002:95). State, politieke entiteite, vyande en vriende word virtuele entiteite wat die spelreëls van intelligensie in alle opsigte verander. Tydens die Koue Oorlog was daar bepaalde grense waarbinne intelligensiegemeenskappe kon funksioneer. Met die einde van die Koue Oorlog het die grense verdwyn en samewerking het oor grense heen tussen intelligensiedienste, private maatskappye en nieregeringsorganisasies plaasgevind. Verder het die ontwikkeling van kommunikasietegnologie tot gevolg gehad dat meer rolspelers tot die internasionale politieke omgewing toegetree het. State is nie meer die enigste en belangrikste rolspelers nie; nieregeringsorganisasies speel ’n groter en toenemende rol, en is trouens soms ’n groter bedreiging as ander state. Grense is nie meer so duidelik waarneembaar nie en state se soewereiniteit word deur nuwe bedreigings in die gesig gestaar. Verder het die verskynsel van sosiale media met behulp van die internet bygedra tot die grenslose wêreld waarbinne ons leef en funksioneer. Ten slotte verwys Rathmell (2002:96) na die kennis-ekonomie waar tegnologiese ontwikkeling, spesifiek kommunikasieontwikkeling, ’n inligtingsekonomie tot gevolg gehad het. Met die magdom van beskikbare inligting moes intelligensiedienste die wyse waarop hulle funksioneer aanpas, veral met betrekking tot die wyse van insameling. Dit is daarom belangrik dat Socmint, as ’n nuwe bron van inligting, ook in die intelligensieproses ingesluit moes word.

Volgens Rathmell se omskrywing van die post-Koue Oorlog-wêreld en die ontwikkeling van die kommunikasietegnologie, is dit noodsaaklik om die nuwe geleenthede en uitdagings wat dit vir intelligensiegemeenskappe tot gevolg het, uit te lig. Dit sluit die volgende in:

https://doi.org/10.56273/1995-5928/2022/j19n2b1

- Intelligensiemededingers: Die inligtingsrevolusie soos meegebring deur die ontwikkeling van inligtingstegnologie (IT) het tot gevolg gehad dat intelligensie nie net meer die gebied van regeringsintelligensiegemeenskappe is nie. Die regeringsintelligensiedienste ding mee met private organisasies (Oxford Analitica, Stratfor en die Institute for Security Studies in Suid-Afrika), akademici en die media.
- Virtuele en grenslose kuberwêreld: Inligtingstegnologie soos die internet het ’n wêreld geskep waar grense nie ’n rol speel nie en waar onwettige aktiwiteite beplan en uitgevoer kan word.
- Waarnemingsvermoëns: Die internet verskaf aan intelligensiedienste die geleentheid vir waarneming om sodoende inligting te verkry. Hierdie geleentheid is egter ook ’n bedreiging. Volgens die Amerikaanse Intelligensiegemeenskapverslag van Februarie 2016 (Clapper 2016:1), is kuber- en tegnologiese ontwikkelings een van die agt bedreigings vir die VSA.
- Inligtingsontploffing: Soos hier bo genoem, het die ontwikkeling van inligtings- en kommunikasietegnologie ’n magdom inligting tot gevolg gehad. Dit bemoeilik die intelligensiewerker se taak om waardevolle inligting te onderskei en te identifiseer. In die era van fopnuus (“fake news”) het dit nog belangriker geword om inligting te sif en te evalueer.
- Gehalte van intelligensieprodukte: Die verskeidenheid tegnologiese ontwikkelings het aan analiste binne die intelligensiegemeenskap die geleentheid gegee om die produkte meer aantreklik voor te berei. Visuele hulpbronne soos interaktiewe kaarte, prente, video’s en foto’s kan ingesluit word in die produkte.
- Die bestuur van menslike bronne (Humint): Wettering (2002:345–9) is van mening dat die internet ’n belangrike medium is om menslike bronne te identifiseer, te werf en te bestuur.

Uit bogenoemde is dit duidelik dat dit vir intelligensiedienste noodsaaklik is om aan te pas met betrekking tot tegnologiese ontwikkelings, wat ook sosiale media insluit, ten einde toepaslik te bly. Die verslag[3] oor die Julie 2021-onrus ondersteun hierdie punt in een van die algemene gevolgtrekkings:

It goes without saying that the capacity of the security services needs to be strengthened to respond effectively to all situations. The security services must use all the lawful levers available to them, in particular the need to intercept communications, in a lawful manner, where the security of the State is at stake. They need to strengthen their technological capacity as well. (Africa, Sokupa en Gumbi 2021:49)

Met inagneming van die bogemelde word Socmint en sosiale media vervolgens in meer besonderhede bespreek.

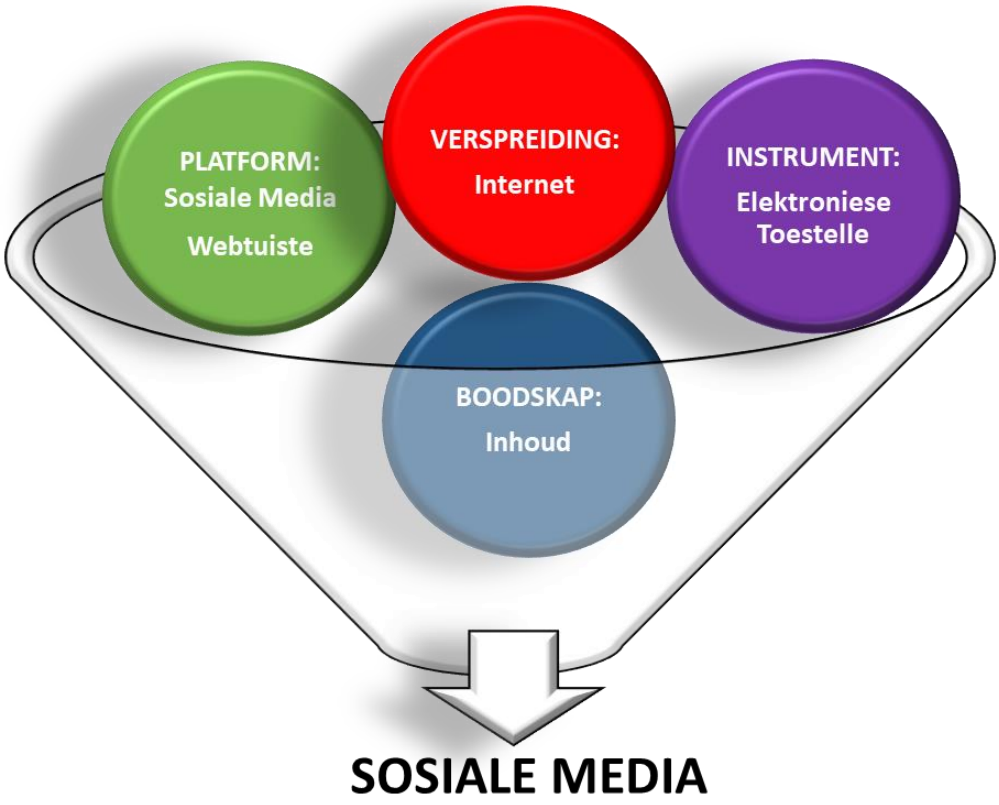
https://doi.org/10.56273/1995-5928/2022/j19n2b1

5. Sosiale media en Socmint

5.1 Omskrywing van sosiale media

Hoewel sosiale media reeds meer as twee dekades lank deel van ons lewe is, is daar steeds geen algemeen aanvaarde definisie vir die begrip nie. Volgens Boyd (2009:1) is sosiale media die sagteware wat gebruikers in staat stel om te kommunikeer, inligting te deel en saam te werk. Nations (2021) en Cohn (2011:1) beskryf sosiale media as platforms wat aanlyn tegnologie vir interaktiewe dialoog gebruik. Ander beskryf sosiale media kortliks as media wat gebruik word om sosiaal te verkeer (Safko 2012:3). Na aanleiding van die verskillende definisies beskryf Stegen (2019:193) sosiale media as: "The set of web-based broadcast technologies that enables people to communicate and to develop from consumers of content to creators of content."

Teen die agtergrond van hierdie definisie is dit duidelik dat die begrip *sosiale media* uit verskillende komponente bestaan. Die eerste komponent is die internet. Die internet is die wyse waarop sosiale media versprei word; die voertuig vir die verspreiding daarvan. Die volgende komponent is die toestel of instrument waarmee sosiale media versprei word, byvoorbeeld selfoon, rekenaar of tabletrekenaar. Sosiale-media-platforms is die derde komponent. Dit sluit platforms soos Facebook®, Instagram™ en Twitter® in. Die laaste komponent is die boodskap, wat verwys na die inhoud van die sosiale-media-plasing. Die komponente word in figuur 2 uiteengesit.



Figuur 2. Komponente van sosiale media

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Sosiale media het sekere eienskappe wat meebring dat dit ’n bydrae tot grootdata lewer. Hierdie eienskappe, wat oorvleuel met dié van die internet, sluit die volgende in (Safranek 2012:2, Omede 2015:275):

- Interaktiwiteit: Sosiale media verskaf aan gebruikers die geleentheid om gesprekke te voer, asook inligting en menings uit te ruil. Hierdie nuwe mediavorm is nie meer bloot eenrigtingkommunikasie nie. Die inligting wat uit hierdie gesprekke verkry word, kan vir die intelligensiegemeenskap waardevol wees.
- Beskikbaarheid en toeganklikheid: Inligting wat geplaas word, is onmiddellik en aan ’n wye groep mense beskikbaar.
- Goedkoop: Gebruikers hoef nie groot uitgawes aan te gaan om toegang tot sosiale media te hê nie.
- Gebruikersvriendelik: Gebruikers kan met ’n minimum tegnologiese kennis die toepassings gebruik.
- Gebrekkige sensorskap: Gebruikers kan inligting versprei sonder om aan die sensorskap en beheer van die regering blootgestel te word. Inligting kan versprei word sonder om dit te verifieer. In die huidige omgewing is dit die gebrek aan sensorskap wat veroorsaak dat fopnuus versprei kan word. Hoewel sekere lande (veral in die COVID-19-tydperk) begin het om boetes teen fopnuus in te stel, is dit nie maklik om die oorsprong daarvan vas te stel of gebruikers/oortreders te vervolg nie.

Sosiale media word gekenmerk deur die vinnige en goedkoop verspreiding van inligting. As gevolg van die menslike drang om deurentyd te kommunikeer is die sosiale-media-platforms voortdurend besig om te groei. Die groei in die gebruik van sosiale media het ook meegebring dat die sekerheids- en wetstoepassingsorganisasies toenemend die inligting op sosiale-media-platforms gebruik om inligtingsbeelde saam te stel (Socmint). Die begrip *Socmint* is vir die eerste keer in 2012 in ’n artikel deur Omand, Bartlett en Miller (2012b) gebruik. In die artikel beskryf die skrywers Socmint as intelligensie wat vanuit sosiale media verkry word (2012b:802).

Socmint word in toenemende mate as ’n waardevolle bron van sekerheidsinligting beskou (Rønn en Søe 2019:362) en word as ’n tipe intelligensie gebruik tesame met ander bronne soos Humint, Osint en Sigint (Lombardi, Rosenblum en Burato 2016:1). Die belangrikheid van Socmint in die intelligensiegemeenskap is ook besig om toe te neem. Marcellino, Smith, Paul en Skrabala (2017:iii) verduidelik dat “the role of social media in military information operations is increasing because the users (allies and adversaries) are sharing information and influencing other users through social media platforms”. Schwab (2016:77) identifiseer sosiale media as een van die tegnologiese ontwikkelings wat die internasionale sekerheidsomgewing transformeer.

Die internet en sosiale-media-platforms het gemeenskappe geskep wat gemaklik daarmee is om hulle inligting aanlyn te deel. Inligting op YouTube™, Twitter® en Facebook® verskaf waardevolle taktiese inligting aan die intelligensiegemeenskap. Hierdie inligting kan aandui wat ’n persoon se gewoontes is, sy/haar belangstellings, groepe wat hy/sy ondersteun, die persoon se kontakte asook die stemming onder die publiek. Hierdie inligting wat op sosiale-media-platforms beskikbaar is, kan ontgin en ontleed word om sodoende Socmint te verkry.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Sosiale media word toenemend deur intelligensiegemeenskappe gebruik om inligting te verkry. Hoewel intelligensiegemeenskappe traag was om sosiale media te gebruik in die insameling van inligting, het gebeure[4]soos die terroriste-aanval in Moembai in 2008, die Groen Revolusie in Iran (2009), die Arabiese Lente in 2010 en protesaksies in Londen (2011), die gemeenskap gedwing om te herbesin.

Om die magdom van inligting op sosiale media te ontgin, is sagteware nodig wat die gebruiker met die volgende kan help (Marcellino e.a. 2017:7–8):

- Die ontleding van sleutelelemente en betekenisvolle taal. Deur die inligting te ontleed kan beplande gebeure geïdentifiseer word.
- Ontleding van sentimente.
- Identifisering van verhoudings (netwerkanalise).
- Vertalings.

Oor die laaste 20 jaar het sosiale media die voorkeurfasiliteerder en -verspreider van inligting geword. Dit het deel van elke aspek van ons daaglikse bestaan geword en het gevolglik ook implikasies vir nasionale veiligheid. In die bespreking hier onder word die implikasies in detail bespreek en verduidelik hoekom Socmint ’n belangrike bron van inligting vir intelligensiedienste is.

5.2 Socmint: bedreigings en geleenthede van sosiale media

Die implikasies van sosiale media kan verdeel word in bedreigings en geleenthede vir nasionale veiligheid. Dover (2020:216) verwys na die bewapening van sosiale media en omskryf dit as:

> […] the transformation of it into a source of potentially actionable intelligence and societal insight and also the transformation of it to become an active security threat.

Hy (2020:216) verdeel die bedreigings in drie groepe. Die eerste is lokalisering van geweld, waar sosiale media gebruik word om protes, geweld en onenigheid teweeg te bring en aan te vuur. Intelligensie-organisasies kan op hulle beurt weer die proses uitbuit deur byvoorbeeld deel van die groep te word en sodoende inligting te bekom. ’n Tweede groep is kollektiewe aksies wat op nasionale of streeksvlak groepe organiseer. Die onlangse #ImStaying wat in 2019 begin is, is ’n voorbeeld in hierdie verband. Die derde groep is die inligtingkonflikte soos gemanifesteer het tydens die 2016- presidensiële verkiesing in die VSA.

Terwyl Dover slegs op protesaksies fokus, het Stegen (2019:200–3) ’n wyer fokus gehad en meer kategorieë geïdentifiseer. Een van die grootste bedreigings van sosiale media is dié van terrorisme. Baie terroriste en ekstremistegroepe gebruik die internet en sosiale-media-toepassings soos Facebook® en YouTube™ vir publisiteit, propaganda, data-ontginning, fondsinsameling, werwing, mobilisering, deel van inligting, beplanning en koördinering van aktiwiteite (Senekal 2018:4, Saxena 2020). Die inligting kan anoniem, vinniger en onder ’n magdom mense versprei word.

Kriminele aktiwiteite is ’n volgende bedreiging vir nasionale veiligheid. Die aktiwiteite sluit in kinderpornografie, dwelmsmokkelary, mensehandel, geldwassery, industriële spioenasie en elektroniese identiteitsdiefstal. Hierdie aktiwiteite het in die laaste aantal jare toegeneem omdat

https://doi.org/10.56273/1995-5928/2022/j19n2b1

die kans dat oortreders gevang sal word, beperk is. Sosiale media vereis dat gebruikers baie van hulle persoonlike inligting verklaar. Hierdie inligting word vir elektroniese identiteits-diefstal gebruik (Von Solms 2013:111).

'n Derde en belangrike bedreiging is protesoptredes en revolusie. Sedert die Arabiese Lente het die rol van sosiale media met betrekking tot protesoptredes baie aandag in die media ontvang. Hoewel sosiale media alleen nie sosiale onrus en revolusies veroorsaak nie, speel dit tog 'n groot rol in die organisering van genoemde aksies. Sosiale media is 'n goedkoop metode om 'n groot groep mense te bereik. Die plaaslike gebeure van Julie 2021 is 'n sprekende voorbeeld van hoe sosiale media ingespan kan word en mense tot oproerigheid en geweld kan aanspoor. Die ondersteuners van Zuma het na sy inhegtenisname boodskappe op sosiale media versprei wat 'n beroep gedoen het om onder andere die land onregeerbaar te maak en president Ramaphosa te onttroon (Africa e.a. 2021:49). Volgens die verslag het sosiale media 'n integrale rol in die onrus gespeel, maar die intelligensiegemeenskap kon nie die inligting verwerk, interpreteer en vir beplanning gebruik nie (Africa e.a. 2021:116). In hierdie verband het die intelligensiegemeenskap erken dat hulle die mag van sosiale media onderskat het (Peter 2021). Die Centre for Analytics and Behavioural Change het in 2021 'n verslag gepubliseer waarin hulle die Radikale Ekonomiese Transformasie-groep (Radical Economic Transformation; RET) ontleed (Mokoka 2021). Die RET het ongeveer 50 Twitter®-rekeninge wat misleidende en verkeerde/valse inligting aanlyn versprei om Zuma en ander politici wat van korrupsie aangekla word, te ondersteun (Mokoka 2021). Vier van die top 20 rekeninge wat geïdentifiseer is as die aanhitsers van die onrus in Julie 2021, behoort aan die RET-groep (Mokoka 2021). Dit is dus duidelik dat protesoptredes soos georganiseer deur sosiale media ook 'n bedreiging vir Suid-Afrika inhou.

'n Volgende bedreiging is fopnuus. Volgens Kapp (2017) is fopnuus "nuus wat versprei word met die doel om lesers te mislei". Hierdie onderwerp het tydens die 2016- presidensiële verkiesing in die VSA sterk op die voorgrond getree. Gedurende die COVID-19-pandemie is verskeie fopnuusboodskappe met betrekking tot die effektiwiteit van entstowwe gestuur. Fopnuus word in baie gevalle in propagandaveldtogte gebruik. In hierdie verband en in 'n poging om fopnuus wat met COVID-19 verband hou te voorkom, het Suid Afrika in Maart 2020, met die afkondiging van die ramptoestand, 'n regulasie (Regulasie 11–5) afgekondig wat dit onwettig maak om enige boodskap op sosiale media te versprei wat mense ten opsigte van COVID-19-verwante aspekte mislei (Suid-Afrika 2020:24).

Voorafgaande bespreking is op die bedreigings wat sosiale media kan inhou, toegespits. Dit is egter belangrik om aan te dui dat sosiale media ook waardevolle geleenthede vir nasionale veiligheid en daarom vir die intelligensiegemeenskap inhou. Skare-verkryging-inligting ("crowd-sourcing information") is inligting rakende spesifieke noodgevalle wat die gemeenskap na regeringsinstansies stuur. Hierdie inligting stel die betrokke instansies in staat om reddingsaksies te beplan. In Junie 2017, tydens die Tuinroete-brande, is sosiale media gebruik om inligting te versprei en reddingspogings te koördineer (Lendrum 2019). Op dieselfde wyse is sosiale media in 2021 deur inwoners in klein dorpies in KZN gebruik om inligting rakende aksies te versprei om hulle dorpe te beskerm.

'n Volgende belangrike aspek is om navorsing te doen oor toepassings en die kommunikasie op die toepassings. Die navorsingsinligting kan help om politieke en radikale groeperings beter te verstaan. So byvoorbeeld is die inligting op sosiale media wat tydens die Julie-onrus van 2021 verskyn het, bestudeer en gebruik om die organiseerders en verspreiders van inligting vas

https://doi.org/10.56273/1995-5928/2022/j19n2b1

te trek (Karombo 2021). Volgens minister Bheki Cele is daar drie persone gearresteer wat na bewering geweld en plundering op sosiale media aangehits het (Zeeman 2021).

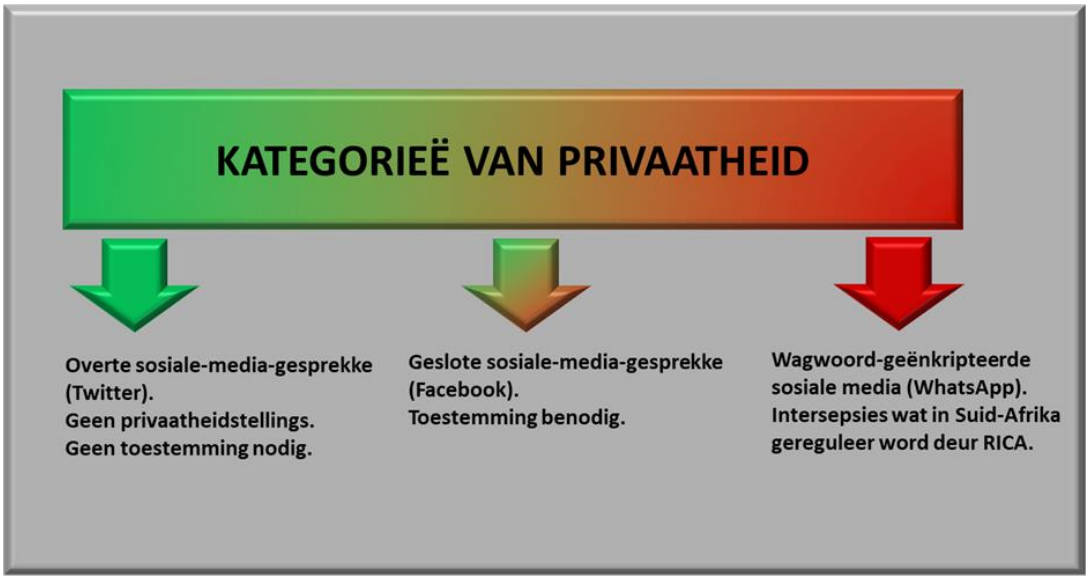
Net soos sosiale media deur individue en groepe gebruik kan word om te beïnvloed, kan regeringsinstellings soos intelligensiedienste dit ook gebruik. Hierdie instellings kan mense se politieke keuses en optredes deur middel van sosiale media beïnvloed. Gedurende die pandemie het die SA-regering sosiale media gebruik om mense aan te moedig om ingeënt te word. So is die veldtog #Grandkidsforgogos gebruik om bejaardes te help om vir die entstof te registreer (Williams 2021).

Laastens kan sosiale media tydens politieke veldtogte as ’n meganisme gebruik word. In hierdie verband was president Obama van die VSA die eerste president wat dit suksesvol gebruik het tydens sy veldtog in 2008 en weer in 2012 (Bogost 2017).

Die mees onlangse tegnologiese ontwikkeling, die internet, het die inligtingsontploffing tot gevolg gehad, in ’n groot mate gedryf deur sosiale media. Dit is dus duidelik uit hierdie bespreking dat sosiale media waardevolle inligting kan verskaf. Hoewel Socmint van groot waarde kan wees, is daar wel uitdagings met betrekking tot dié bron van inligting.

5.3 Socmint as uitdaging vir die intelligensie-omgewing

Bostaande bespreking het gefokus op die gebruik en voordele van Socmint binne die intelligensie-omgewing. Daar is egter uitdagings waaraan aandag geskenk moet word wanneer Socmint gebruik word. Die eerste, wat al meer na vore kom in debatte oor die gebruik van sosiale media vir intelligensie, is die wetlike aspek daarvan (Omand, Bartlett en Miller 2014:36). Volgens Omand, Bartlett en Miller (2012a) is daar drie kategorieë van toegang (sien figuur 3 hier onder). Die eerste is oop sosiale media wat in die openbare domein toeganklik is. Die tweede is gedeeltelik-privaat – toegang tot hierdie inligting kan slegs verkry word deur ’n lid van die gemeenskap of groep te word. Die derde kategorie is geheim en impliseer onderskeppings. Toegang kan slegs met wettige toestemming verkry word.



Figuur 3. Socmint-kategorieë van privaatheid
Bron: Aangepas vanuit Omand, Bartlett en Miller 2012a

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Die meeste lande het wetgewing wat onderskeppings/afluistering reguleer. Hierdie wetgewing is egter voor sosiale media ingestel. Televisie en die geskrewe media is deur die regering gereguleer en het in die meeste gevalle verantwoording aan die regering van die dag gedoen. Die tegnologierevolusie bemoeilik die regulering van inligting. Dit is onmoontlik om die internet te beheer en te polisieer. Tydens die studente-onrus in 2017 het die minister van staatsveiligheid, David Mahlobo, opgemerk dat die regulering van sosiale media in Suid-Afrika ondersoek moet word (Pierce 2017). Hierdie opmerking het onmiddellike reaksie op sosiale media uitgelok met #HandsOffSocialMedia, waar verskeie lede van die sosiale-media-gemeenskap hulle ontevredenheid oor die moontlikheid van regulering in die sosiale-media-omgewing uitgespreek het (Van der Merwe 2017:1). Gevalle waar lande internettoegang beperk of selfs heeltemal afsluit, is aan die toeneem. Selfs in Suid-Afrika is daar tydens die 2015-opening van die parlement toestelle gebruik om te verhoed dat die media boodskappe op selfone kon stuur en ontvang (Gilbert 2016). In 2016 het die hof hierdie aksies as onwettig verklaar. Verskeie lande in Afrika het in die onlangse verlede die internet of sosiale-media-toepassings geblokkeer (Giles en Mwai 2021, Armstrong 2022):

- In Oktober 2020 het Tanzanië tydens die verkiesings toegang tot sosiale media beperk.
- In Junie 2020 het Ethiopië die internet vir byna ’n maand heeltemal afgesluit in reaksie op onrus wat op die dood van die sanger Hachalu Hundessa gevolg het.
- Zimbabwe, Togo, Burundi en Mali het almal in 2020 op die een of ander stadium die internet of sosiale media geblokkeer.
- Burkina Faso het in Januarie 2022 tydens die beweerde coup d’état die sosiale-media-toepassings ontwrig.

Dit is ook belangrik om hier te verwys na ’n ander debat oor Socmint, naamlik die verhouding tussen Osint en Socmint. Sommige is van mening dat Socmint as ’n verlenging of onder-afdeling van Osint beskou moet word (Kolb 2020). Ander is weer oortuig dat Socmint ’n afsonderlike dissipline is (Senekal 2018:8). Die aspek wat dit bemoeilik, is dat Socmint as oop (in die openbare domein beskikbaar) of geheim (nie beskikbaar in die openbare domein nie) geklassifiseer kan word (Bartlett en Miller 2013:14). Voor die internet is Osint geklassifiseer as “information, lawfully obtained from overtly available sources such as newspapers, journals, books, conferences and government reports” (DCAF 2006:2; Liaropoulos 2013:10). Met die ontwikkeling van die internet en die rekenaar is die definisie aangepas om rekenaargebaseerde inligting in te sluit (Lowenthal 2006:101). Wat is dan die verskil tussen Socmint en Osint? Volgens Bartlett en Miller (2013:14) is die verskil geleë in die inhoud en die ingewikkelde vaardighede wat nodig is om die inligting te ontleed. Senekal (2018:8) is van mening dat Socmint afsonderlik van Osint beskou moet word omdat dit binne ’n grootdataparadigma gesetel is. Teen hierdie agtergrond stem ons saam met Senekal dat Socmint verskil van Osint en daarom as ’n afsonderlike dissipline beskou moet word.

Die tweede uitdaging van Socmint is die geloofwaardigheid daarvan (Omand, Bartlett en Miller 2014:33). Socmint is ’n nuwe tipe intelligensie, en tot dusver is daar geen kriteria om die geloofwaardigheid hiervan te toets nie. Voordat inligting gebruik en verwerk kan word, is verifikasie en die bepaling van die oorsprong daarvan baie belangrik. ’n Volgende uitdaging is verteenwoordiging (Omand, Bartlett en Miller 2014:33). Sagteware word gebruik om die magdom inligting te ontgin, maar omdat sosiale-media-gebruikers nie verteenwoordigend van die totale wêreldbevolking is nie, kan die data nie geëkstrapoleer word en van toepassing gemaak word op die groter populasie nie. Nog ’n uitdaging is akkuraatheid (Omand, Bartlett

https://doi.org/10.56273/1995-5928/2022/j19n2b1

en Miller 2014:34). Die sagteware wat gebruik word om die data te ontgin is betreklik nuut. Die akkuraatheid van die toepassing kan alleen met verloop van tyd bepaal word. ’n Volgende uitdaging wat met bogenoemde saamhang, is egtheid (Omand, Bartlett en Miller 2014:34). Anonimiteit op die internet, spesifiek met betrekking tot sosiale media, skep ’n ideale geleentheid vir misleiding. Dit is besonder moeilik om inligting wat aanlyn beskikbaar is te verifieer. Dit is ook om hierdie rede dat daar so baie fopnuus op sosiale media verskyn. ’n Sesde uitdaging is realiteit (Omand, Bartlett en Miller 2014:33). Inligting wat in sosiale-media-toepassings ontgin word, verskaf geen konteks nie. Om bruikbaar te wees, moet die inligting eers in konteks geplaas word. ’n Laaste uitdaging is die stawing van inligting (Omand, Bartlett en Miller 2014:33). Daar is tans geen wyse om die inligting wat op sosiale media verskyn, te staaf nie.

Hoewel Socmint verskeie uitdagings bied en spelreëls herdefinieer en herbepaal (soos hier bo verduidelik), is dit tog van belang vir die intelligensiegemeenskap en kan dit van groot waarde wees vir hierdie instellings in die uitvoering van hulle pligte.

5.4 Intelligensiewaarde van sosiale media

Die intelligensiewaarde van sosiale media kan gemeet word aan die verskillende gebeure wat die afgelope twee dekades plaasgevind het. In 2001 het ’n sosiale-media-veldtog in die Filippyne bygedra tot president Estrada se bedanking (Shirky 2011:1). Tydens die terroriste-aanval van 2008 in Moembai het inwoners die polisie se bewegings op Twitter® versprei, wat die polisie se pogings bemoeilik het (Thompson 2011:177). In 2009 het onrus in Moldawië uitgebreek nadat die opposisie die regerende party van bedrog beskuldig het (Safranek 2012:3). Die onrus het daartoe bygedra dat ’n tweederondte-verkiesing gehou is, wat deur ’n koalisie van opposisiepartye gewen is (Dix 2011:93). Die Iranse Groen Revolusie in 2009 was die eerste groot gebeurtenis wat sosiale media gebruik het om internasionale aandag op die situasie in die land te plaas (Liaropoulos 2013:8). In Desember 2010 het sosiale media gehelp om die situasie in Tunisië onder die internasionale gemeenskap se aandag te bring (Safranek 2012:3). Die onrus in Tunisië is gevolg deur die onrus in Egipte. Die burgers in Egipte het teen die onderdrukking en korrupsie van president Mubarak se regering betoog (Liaropoulus 2013:9). ’n Kombinasie van nuwe media (sosiale media) en tradisionele media (TV) het die onderdrukking in Egipte onder die aandag van die internasionale gemeenskap gebring.

Bogenoemde gebeure het die volgende geleenthede vir die intelligensiegemeenskap gebied: In al die gevalle kon sosiale media die intelligensiegemeenskap help om die gesindheid onder die bevolking te bepaal. Ontleding van die inligting sou kon aantoon dat die bevolking ongelukkig met die regering en ongeduldig met die situasie was. In die Moembai-aanval kon die polisie die burgers se inligting gebruik om ’n beeld te vorm van waar die aanvallers was. Die belangrike rolspelers kon geïdentifiseer word deur hulle ligging en sosiale netwerke te ontleed. ’n Deeglike ontleding van sosiale media sou moontlik die gebeure kon identifiseer en voorkom.

Sosiale media het in bogenoemde gevalle nie die gebeure veroorsaak nie, maar het ’n bepaalde rol gespeel om die optredes meer effektief te maak. Die onderliggende sosio-ekonomiese en politieke situasies in die gemelde lande het die gebeure veroorsaak en sosiale media het dit aangevuur. Verder het sosiale media ’n deurslaggewende rol gespeel om die boodskap aan die begin van die opstande te versprei, die optredes te organiseer, asook om die internasionale gemeenskap bewus te maak van die toestande in die onderskeie lande. Laastens het sosiale media die voorkoms van joernalistiek verander. Enige persoon met ’n selfoon en toegang tot

https://doi.org/10.56273/1995-5928/2022/j19n2b1

die internet kan nou ’n joernalis wees. Die digitale toepassings kan nou gebruik word om inligting na mense regoor die wêreld te versprei.

6. Ten slotte

Intelligensie se rol en funksie het oor die jare heen onveranderd gebly, naamlik om nasionale veiligheid te verseker. Die omgewing waarbinne hierdie taak uitgevoer moet word, is nie staties nie en verander voortdurend. Dit beklemtoon die belangrikheid van ’n aanpasbare organisasie. Die konteks of omgewing waarbinne die intelligensie-organisasies optree het veral na die Koue Oorlog vinnig en voortdurend verander. Tans word die wêreld gebombardeer met veranderings op politieke, ekonomiese, sekerheids- en sosiale vlak. Die grootste dryfveer van hierdie veranderings is die ontwikkeling en groei van die inligtings- en kommunikasietegnologie.

Die nuwe sekerheidsomgewing, soos geskep deur die nuwe en snel veranderende kommunikasietegnologie en die einde van die Koue Oorlog, het bepaalde uitdagings vir die intelligensiegemeenskap tot gevolg. Een van die grootste veranderings is die mededinging met private organisasies vir die lewering van intelligensie. Intelligensie-organisasies het nie meer die eksklusiewe reg om intelligensie te verskaf nie. Hierdie mededinging dwing regerings se intelligensiedepartemente om hulle werkswyses op te skerp. ’n Verdere uitdaging is die insameling van inligting wat deur die nuwe tegnologie geraak word en wat direk tot die intelligensiesiklus spreek. Die insameling van intelligensie het verskuif van ’n hoofsaaklik fisiese omgewing tot ’n kombinasie van fisiese en kuberruimtes. Hierdie veranderde omgewing het die intelligensiegemeenskap genoodsaak om werkswyses ten opsigte van insameling aan te pas. Tradisionele bronne van inligting is nie meer voldoende om ’n volledige inligtingsbeeld te gee nie, veral nie weens nuwe bedreigings vir nasionale veiligheid nie. Dit is verder ook belangrik dat, in die huidige omgewing van massa-inligting, intelligensiegemeenskappe nie nietig moet raak nie. Die evolusie van intelligensie wat in die Tweede Wêreldoorlog begin is, moet voortgesit word, en intelligensie-organisasies sal slegs betekenisvol bly as hulle by tegnologiese ontwikkelings aanpas. In hierdie opsig is dit noodsaaklik dat alle bronne van inligting ingesamel en noukeurig vertolk moet word. Die ondersoek van nuwe bronne van inligting, soos Socmint, is dus noodsaaklik.

Beleidmakers werk wêreldwyd in ’n omgewing waar dit noodsaaklik is dat die tyd tussen besluitneming en implementering (“real-time”) so kort as moontlik moet wees (Andrus 2005:1). Die veranderings in die tegnologie vind baie vinniger plaas as die veranderings in die sekerheids- en intelligensie-omgewings. Dit is dus uiters belangrik dat ’n regering oor die nuutste inligting moet beskik, sodat korrekte besluite rakende implementering van beleid geneem kan word. Uit die artikel is dit duidelik watter rol Socmint in die proses kan speel en dat dit bygedra het tot die evolusie van hedendaagse intelligensie. Dit is daarom van groot belang dat die essensie van die nuwe bron ten volle verstaan word, sodat dit by die intelligensieproses ingesluit kan word. Deur inligting uit sosiale media te vertolk en by die finale produk in te sluit, kan die inligtingsbeeld verbeter word, wat die nasionale kliënt met beleidsbesluite kan bystaan.

Die verskuiwingslyne wat aanpasbaarheid binne die Suid-Afrikaanse intelligensiegemeenskap betref, is duidelik aangetoon deur die staatskapingsage, en nog duideliker tydens die onrus wat in Julie 2021 uitgebreek het. Vroeër in die artikel is die funksie van intelligensie bespreek,

https://doi.org/10.56273/1995-5928/2022/j19n2b1

naamlik om te waarsku, in te lig en te voorspel. Gemeet aan hierdie kriteria, kan die gebeure van Julie 2021 as ’n algehele mislukking van intelligensie beskryf word. Die intelligensiegemeenskap het nie die vermoë (menslike of tegniese hulpbronne) gehad om besluitnemingsinligting aan die staatspresident te verskaf nie. In die aanloop tot die gebeure is sosiale media breedvoerig gebruik om mense tot aksie aan te spoor. Die intelligensiegemeenskap het dit nie agtergekom nie.

Hoewel sosiale media as ’n instrument van vroeë waarskuwing kan dien, word dit nie binne die Suid-Afrikaanse omgewing as sodanig gebruik nie. Dit blyk duidelik uit die gebeure van Julie 2021. Indien hierdie bron van inligting met die nodige erns en respek hanteer was, sou die gebeure van 2021 baie meer doeltreffend die hoof gebied kon word.

Om die voorkeurverskaffer van inligting vir nasionale veiligheid te wees, sal die Suid-Afrikaanse intelligensiegemeenskap die volgende aspekte in aanmerking moet neem:

- Die gemeenskap sal vinniger by die huidige hoofsaaklik tegnologiese omgewing moet aanpas.
- ’n Paradigmaskuif ten opsigte van insameling sal binne die gemeenskap moet plaasvind, toegespits op beide tradisionele bronne (menslike bronne) en nuwe tegnologiese bronne (sosiale media).
- Die nuwe omgewing waarin die intelligensiegemeenskap bedryf word, is sterk ingestel op tegniese kennis. Nuwe vaardighede met betrekking tot die monitering van sosiale media sal geprioritiseer moet word.
- Nuwe strategieë ten opsigte van werwing (bronne en lede), insameling, navorsing en verwerking van inligting sal ontwikkel moet word.
- Dit is van uiterste belang dat die intelligensiegemeenskap oor die nuutste tegnologie moet beskik. Hierdie tegnologie moet in staat wees om sosiale media te ontleed en voorkennis te verskaf.
- Ondersoek moet ingestel word na samewerkingsooreenkomste met private maatskappye wat kan help met sagteware vir die ontleding van sosiale media.
- Sommige lande beskik oor groot afdelings wat Socmint beskou en bestudeer. Dit is noodsaaklik dat die Suid-Afrikaanse intelligensiegemeenskap die tendens navolg en ook ’n afdeling op die been bring wat in Socmint spesialiseer.

Een van die grootste redes vir die onlangse mislukking van intelligensie is die feit dat die intelligensiegemeenskap nie vinnig genoeg aangepas het by die huidige oorwegend tegnologiese en virtuele konteks nie. Dit is van uiterste belang dat die gemeenskap leer om in hierdie konteks te werk, anders sal dit nie die laaste mislukking van intelligensie wees nie. In Suid-Afrika word sosiale media toenemend gebruik om ondersteuning vir sekere optredes te loods (#feesmustfall, #zumamustfall). Is dit nie hoog tyd dat die intelligensie uit Socmint verkry, sy volwaardige plek binne intelligensie moet inneem nie?

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Bibliografie

Adas, M. (red.). 2010. *Essays on twentieth century history*. Philadelphia: Temple University Press.

Africa, S., S. Sokupa en M. Gumbi. 2021. Report of the Expert Panel into the July 2021 civil unrest. 2021. https://www.thepresidency.gov.za/content/report-expert-panel-july-2021-civil-unrest (7 Februarie geraadpleeg).

Armstrong, M. 2022. Where social media is suppressed. https://www.statista.com/chart/23804/countries-blocking-social-media (8 Februarie 2022 geraadpleeg).

Andrus, D.C. 2005. The Wiki and the Blog: Toward a complex adaptive intelligence community. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904 (14 Desember 2021 geraadpleeg).

Baker, J. 2018. Forgotten heroes of the Enigma story. https://www.nature.com/articles/d41586-018-06149-y (14 Desember 2021 geraadpleeg).

Bogost, I. 2017. Obama was too good at social media. https://www.theatlantic.com/technology/archive/2017/01/did-america-need-a-social-media-president/512405 (13 Desember 2021 geraadpleeg).

Boyd, D.M. 2009. Social media is here to stay. Now what? http://www.danah.org/papers/talks/MSRTechFest2009.html (13 Desember 2021 geraadpleeg).

Breakspear, A. 2013. A new definition of intelligence. *Intelligence and National Security*, 28(5):678–93.

Clapper, J. 2016. Worldwide threat assessment of the US intelligence community. https://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf (15 Desember 2021 geraadpleeg).

Classen, J.S. 2005. The craft of intelligence analysis and assessment: A training manual for intelligence analysts. Ongepubliseer (in eie besit).

Cohn, M. 2011. Social media vs. social networking. https://www.compukol.com/social-media-vs-social-networking (15 Desember 2020 geraadpleeg).

Cox, K., W. Marcellino, J. Bellasio, A. Ward, K. Galai, A.S. Meranto en G.P. Paoli. 2018. Social media in Africa a double-edged sword for security and development. https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf (6 Februarie 2022 geraadpleeg).

DataReportal. 2021. Digital around the world in 2021. https://datareportal.com/reports/digital-2021-global-overview-report (5 Januarie 2022 geraadpleeg).

DCAF (Democratic Control of Armed Forces). 2003. Intelligence practice and democratic oversight – A practitioner's view. Occasional paper no 3.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

https://www.dcaf.ch/sites/default/files/publications/documents/op03_intelligence-practice.pdf (15 Desember 2021 geraadpleeg).

—. 2006. Intelligence services – Backgrounder. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf (15 Desember 2021 geraadpleeg).

Die Grondwet van die Republiek van Suid-Afrika – Sien Suid-Afrika.

Dix, H. 2011. Republic of Moldova at the end of an election marathon? https://www.kas.de/c/document_library/get_file?uuid=167aba35-acfb-a584-ebc6-bc941f5a6873&groupId=252038 (15 Desember 2021 geraadpleeg).

Dover, R. 2020. Socmint: A shifting balance of opportunity. *Intelligence and National Security*, 35(2):216–32.

Duncan, J. 2017. How state spying enables state capture. https://www.dailymaverick.co.za/article/2017-08-17-op-ed-how-state-spying-enables-state-capture (6 Februarie 2022 geraadpleeg).

Ferris, J. 1988. The British army and signals intelligence in the field during the First World War. *Intelligence and National Security*, 3(4):23–48.

Gartner, 2016. What is big data? – Gartner IT Glossary – Big Data. http://www.gartner.com/it-glossary/big-data (20 Maart 2021 geraadpleeg).

Gilbert, P. 2016. SONA signal jamming "unlawful". https://www.itweb.co.za/content/3mYZRXv9OAGMOgA8 (8 Februarie 2022 geraadpleeg).

Giles, C. en P. Mwai. 2021. Africa internet: Where and how are governments blocking it? https://www.bbc.com/news/world-africa-47734843 (8 Februarie 2022 geraadpleeg).

Gill, P. en M. Phythian. 2006. *Intelligence in an insecure world.* Cambridge: Polity Press.

Hecht, G. en P.N. Edwards. 2010. The techno politics of the Cold War. In Adas (red.) 2010.

Hobbs, C., M. Moran en D. Salisbury (reds.). 2014. *Open source intelligence in the twenty-first century: New approaches and opportunities.* Hampshire: Macmillan.

Hunter, Q., J. Wicks en K. Singh. 2021. *Eight days in July: inside the Zuma unrest that set South Africa alight*. Kaapstad: Tafelberg Uitgewers.

Internet Society. 2016. Internet invariants: What really matters. An internet society public policy briefing. https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetInvariants-20160926-nb.pdf (20 Desember 2021 geraadpleeg).

Johnson, L.K. 2009. Sketches for a theory of strategic intelligence. In Gill e.a. (reds.) 2009:33–53.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Kahn, D. 2006. The rise of intelligence. *Foreign Affairs*, 85(5):125–34.

Kapp, S. 2017. Fopnuus. https://viva-afrikaans.org/lees-luister/blog/item/267-fopnuus (20 Desember 2021 geraadpleeg).

Karombo, T. 2021. South Africa goes after social media as it cracks down on looting and protests. https://qz.com/africa/2033328/south-africa-to-monitor-social-media-as-protests-rock-the-country (6 Februarie 2022 geraadpleeg).

Kent, S. 1966. *Strategic intelligence for American world policy*. Princeton: Princeton University Press.

Kolb, D. 2020. How to run social media investigations. https://traversals.com/blog/social-media-investigations (29 Desember 2021 geraadpleeg).

Lanz, M. 2019. How the CIA overthrew Iran's democracy in 4 days. https://www.npr.org/2019/01/31/690363402/how-the-cia-overthrew-irans-democracy-in-four-days (6 Februarie 2022 geraadpleeg).

Lendrum, D.A. 2019. How people affected by disaster use social media: A study of Facebook usage during the 2017 Garden Route fires. MPhil-proefskrif, Universiteit Stellenbosch.

Liaropoulos, A. 2013. The challenges of social media intelligence for the intelligence community. *Journal of Mediterranean and Balkan Intelligence*, Januarie:5–14.

Lombardi, M., T. Rosenblum en A. Burato. 2016. From SOCMINT to HUMINT: Re-frame the use of social media within the intelligence cycle. http://www.fondazionedegasperi.org/wp-content/uploads/2016/10/Paper-From-SOCMINT-to-Digital.pdf (29 Desember 2021 geraadpleeg).

Lowenthal, M.M. 2020. *Intelligence: From secrets to policy*. Washington: CQ Press.

Marcellino, W., M.L. Smith, C. Paul en L. Skrabala. 2017. Monitoring social media: Lessons for future Department of Defence social media analysis in support of information operations. https://www.rand.org/pubs/research_reports/RR1742.html (29 Desember 2021 geraadpleeg).

Matilda, S. 2016. Big data in social media environment: A business perspective. https://www.researchgate.net/publication/316665818_Big_Data_in_Social_Media_Environment_A_Business_Perspective (17 Desember 2021 geraadpleeg).

Mokoka, M. 2021. RET's digital war of words: The fake online network hijacking the Twittersphere. https://www.dailymaverick.co.za/article/2021-05-27-rets-digital-war-of-words-the-fake-online-network-hijacking-the-twittersphere (7 Februarie 2022 geraadpleeg).

—. 2021. Meet the instigators: The Twitter accounts of the RET forces network that incited violence and demanded Zuma's release. https://www.dailymaverick.co.za/article/2021-07-25-meet-the-instigators-the-twitter-accounts-of-the-ret-forces-network-that-incited-violence-and-demanded-zumas-release (7 Februarie 2022 geraadpleeg).

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Nations, D. 2021. What is social media. https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616 (5 Junie 2022 geraadpleeg).

Omand, D., D. Bartlett en C. Miller. 2012a. A balance between security and privacy online must be struck. https://www.demos.co.uk/wp-content/uploads/2017/03/intelligence-Report.pdf (4 Junie 2022 geraadpleeg).

—. 2012b. Introducing social media intelligence (Socmint). *Intelligence and National Security Journal*, 27(6):801–23.

—. 2014. Towards the discipline of social media intelligence. In Hobbs, Moran en Salisbury (reds.) 2014.

Omede, A.J. 2015. Social media: A trend or threat to democracy. *Jorind*, 13(1):272–78.

Peter, C. 2021. How social media fuelled the burning and looting. https://www.news24.com/citypress/voices/how-social-media-fuelled-the-burning-and-looting-20210717 (7 Februarie 2022 geraadpleeg).

Pierce, L. 2017. Why regulating social media in South Africa cannot, should not and will not be allowed to happen. https://www.ppmattorneys.co.za/regulating-social-media-south-africa-cannot-not-will-not-allowed-happen (29 Desember 2021 geraadpleeg).

Potts, D.A. 2014. Characteristics of the internet. https://www.cyberlibel.com/?page_id=1549 (12 Desember 2021 geraadpleeg).

Rathmell, A. 2002. Towards postmodern intelligence. *Intelligence and National Security Journal*, 17(3):87–104.

Rønn, K.R. en S.O. Søe. 2019. Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security Journal*, 34(3):362–78.

Safko, L. 2012. *The social media bible: Tactics, tools and strategies for business success*. Hoboken: John Wiley & Sons.

Safranek, R. 2012. The emerging role of social media in political and regime change. http://www.databank.com.lb/docs/The%20Emerging%20Role%20of%20Social%20Media%20in%20Political%20and%20Regime%20Change%20-2012.pdf (12 Desember 2021 geraadpleeg).

Saxena, K. 2020. Social media – a tool for terrorism? https://thesecuritydistillery.org/all-articles/social-media-a-tool-for-terrorism (20 Desember 2021 geraadpleeg).

Senekal, A.B. 2018. Socmint: Die monitering van sosiale media vir gemeenskapsveiligheidsdoeleindes binne ’n grootdataraamwerk in Suid-Afrika met spesifieke verwysing na Orania. https://www.litnet.co.za/wp-content/uploads/2018/12/LitNet_Akademies_15-3_Senekal_276-309.pdf (5 November 2021 geraadpleeg).

Shirky, C. 2011. The political power of social media. *Foreign Affairs*, 13(2):1–9.

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Shulsky, A.N. en G.T. Schmitt. 2002. *Silent warfare: Understanding the world of intelligence*. Dulles: Potomac Books.

START (The National Consortium for the Study of Terrorism and Responses to Terrorism). 2018. The use of social media by United States extremists. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf (20 Desember 2021 geraadpleeg).

Statistica. 2021. Countries with the lowest internet penetration rate as of January 2021. https://www.statista.com/statistics/725778/countries-with-the-lowest-internet-penetration-rate (15 Desember 2021 geraadpleeg).

Stegen, J.I. 2019. Social media intelligence (Socmint) within the South African context: A theoretical and strategic framework for the national security environment. PhD-proefskrif, Noordwes-Universiteit.

Suid-Afrika. 1995. Witskrif oor Intelligensie. https://www.gov.za/documents/intelligence-white-paper (15 Desember 2021 geraadpleeg).

—. 1996. Die Grondwet van die Republiek van Suid-Afrika. Pretoria: Die Staatsdrukker.

—. 2002. Wet op Rampbestuur. https://www.gov.za/sites/default/files/gcis_document/202003/43107gon318.pdf (7 Februarie geraadpleeg).

Thompson, R. 2011. Radicalization and the use of social media. *Journal of strategic security*, 4(4):167–90.

Van der Merwe, M. 2017. State security and social media: Is big brother following you? *Daily Maveric*k. https://www.dailymaverick.co.za/article/2017-03-07-state-security-and-social-media-is-big-brother-following-you (14 Desember 2021 geraadpleeg).

Vaisman, A. en E. Zimanyi. 2014. *Data warehouse systems design and implementation*. Heidelberg: Springer-Verlag.

Warner, M. 2002. Wanted: A definition of “intelligence”. *Studies in Intelligence*, 46(3):15–22.

Wettering, F.L. 2001. The internet and the spy business. *International Journal of Intelligence and Counterintelligence*, 14(3):342–65.

White Paper on Intelligence – sien Suid-Afrika.

Williams, P. 2021. Behind the state’s communications strategy to encourage Covid-19 vaccinations. https://www.gov.za/blog/behind-states-communications-strategy-encourage-covid-19-vaccinations (6 Februarie 2022 geraadpleeg).

Zeeman, K. 2021. Three alleged instigators of violent unrest arrested and expected in court this week. https://www.timeslive.co.za/news/2021-07-18-three-alleged-instigators-of-violent-unrest-arrested-and-expected-in-court-this-week (6 Februarie 2022 geraadpleeg).

https://doi.org/10.56273/1995-5928/2022/j19n2b1

Eindnotas

[1] Stegen, J.I. 2019. Social media intelligence (Socmint) within the South African context: A theoretical and strategic framework for the national security environment. PhD-proefskrif, Noordwes-Universiteit. Hierdie PhD-studie het gepoog om deur middel van ’n diepgaande literatuurstudie (gerig op die verstaan van die gebruik van sosiale media in ’n intelligensie-omgewing [Socmint]) die belangrikheid hiervan as grondslag van inligting en intelligensie in die inligtingsera te beklemtoon. Die PhD-studie was kwalitatief van aard en het vanuit ’n metateoretiese en teoretiese raamwerk die tema op ’n deduktiewe wyse benader. Laasgenoemde beteken dat ’n teoretiese raamwerk ontwikkel is en van toepassing gemaak is op die tema. Die waarde en betekenis vir die Suid-Afrikaanse konteks is hierin sterk beklemtoon. Die hoofdoel van die PhD-studie was dus om ’n strategiese raamwerk te ontwikkel om Socmint as belangrike werkswyse en metodologie vir die verwerwing van strategiese inligting in die Suid-Afrikaanse intelligensiegemeenskap uit te wys en die waarde en betekenis hiervan te bepaal. Verder was daar geen menslike deelname nie en die res van die etiese aspekte is aan voldoen.

[2] Ten einde meer inligting te verkry oor die vroeë ontwikkeling van intelligensie, kan Stegen (2019:135–42) geraadpleeg word.

[3] Op 5 Augustus 2021 het president Ramaphosa ’n paneel aangewys om Suid-Afrika se reaksie op die onrus te ondersoek, met die klem op die paraatheid en tekortkominge. Die paneel het uit drie lede bestaan: professor Sandy Africa (voorsitter), mnr. Silumko Sokupa en advokaat Mojankunyane Gumbi. Die verslag is op 7 Februarie 2022 aan die publiek vrygestel.

[4] Vir ’n volledige bespreking van die gebeure, sien Stegen (2019:212).