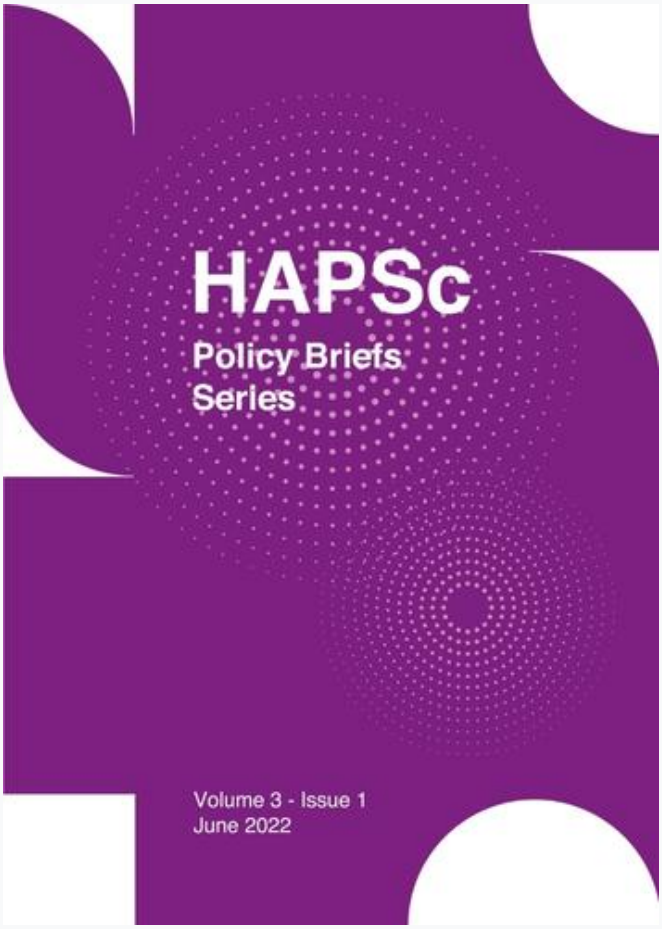
HAPSc Policy Briefs Series

Vol 3, No 1 (2022)

HAPSc Policy Briefs Series



Strategic Social Media Management in Conflict Zones through the Analysis of the Intelligence Cycle: Lessons Learned from the Russo-Ukrainian Conflict

Zisis Kyrgos

doi: 10.12681/hapscpbs.31000

To cite this article:

Kyrgos, Z. (2022). Strategic Social Media Management in Conflict Zones through the Analysis of the Intelligence Cycle: Lessons Learned from the Russo-Ukrainian Conflict. *HAPSc Policy Briefs Series*, *3*(1), 114–120. https://doi.org/10.12681/hapscpbs.31000

 ISSN: 2732-6578 (print version) 2732-6586 (online)

Strategic Social Media Management in Conflict Zones through the Analysis of the Intelligence Cycle: Lessons Learned from the Russo-Ukrainian Conflict[1]

Zisis Kyrgos[2]

Abstract

Social media have become an important aspect of everyday life, especially in the western world. Through the analysis of the Intelligence Cycle and the social media communication process, it is possible to determine how social media are integrated into the intelligence process, namely during the data collection phase, and what types of intelligence vulnerability emerge, namely SIG.INT. and O.S.INT. type vulnerabilities. The recent events of the Russo-Ukrainian conflict have shown that the uneducated use of social media, by civilians and military personnel alike, poses a serious threat to national security in times of conflict. Educating the general public on matters of operations security could be vital to safeguarding national security, a process which could be aided by social media platforms' moderators and AI technology.

Keywords: social media, Russia, Ukraine, conflict, operations security, intelligence operations, security.

Introduction

The role of social media in conflicts is not a novel field of study. Research has shown that social media played an important role in many major conflicts of the 21st century, such as the Arabic Spring (Comunello & Anzera, 2012) and the subsequent Syrian Civil War (Zeitzoff, 2017). However, most of the published research revolves on the subjects of fake news, misinformation, disinformation, propaganda and influence operations; on how the public and information image of an event are shaped in order to promote a political or otherwise ideological end (Viekerk & Maharaj, 2013; Sacco & Bossio, 2015; Zeitzoff, 2016). In the light of the recent events of the Russo-Ukrainian conflict, a new security threat involving social media has been brought back to the stage, namely the unintentional publication of sensitive military data by the public and its exploitation by the opposing side. This paper examines the issue through the prism of a pragmatic approach and the strategic prospective of national security, defining its parameters, the effects it has on national security and a possible approach on confronting the problem.

Defining the Parameters: Social Media and the Intelligence Cycle

Social media's emergence and evolution is closely related to that of the World Wide Web (University of Michigan, 2021). As defined by Kaplan and Haenlein (2010), social media are *"a group of*

[1] To cite this paper in APA style: Kyrgos, Z. (2022). Strategic Social Media Management in Conflict Zones through the Analysis of the Intelligence Cycle: Lessons Learned from the Russo-Ukrainian Conflict. *HAPSc Policy Briefs Series*, *3*(1), 114-120. https://doi.org/10.12681/hapscpbs.31000

[2] M.Sc. Crisis Management, University of Bolton. Researcher at Hellenic Institute for Strategic Studies, Athens, Greece.

Internet-based applications […] that allow the creation and exchange of User Generated Content". This exchange of content is possible to be achieved either as a user-to-user (private) or a user-to-users (public) process. On a global scale, 58.4% of the world's population are social media users, a percentage which amounts to the 93.4% of total internet users, spending an average daily time of 2.5 hours interacting with a social media platform (Chaffey, 2022).

Taking into consideration the wide use of social media, it is only natural that intelligence agencies have shown a great interest in their possible exploitation as a means of achieving their mission. In the context of this research, it is necessary to briefly examine the process through which that is achieved; the process which ultimately connects social media and intelligence.

Western intelligence agencies use a strategically standardized methodology for the collection, analysis and dissemination of information, the *Intelligence Cycle*. The cycle consists of six distinct steps: planning, collection, processing, analysis, dissemination and evaluation. Its purpose is to convert raw collected data into information and finally intelligence products that can be utilized by civilian and military actors in decision-making processes (Phythian, 2013). For the purposes of this research paper, it is not necessary to analyze the entirety of the cycle, but rather focus on the collection step, which is proposed to be the point where social media are integrated into the cycle. There are several collection methods available to intelligence agencies. In this regard, intelligence is categorized into six different types, depending on its source of origin, as explained below (Phythian, 2013):

Geospatial Intelligence or GEO.INT. refers to intelligence secured through data originating from the combination of geographical imagery and other forms of intelligence. *Human Intelligence or HUM.INT.* refer to data collected from various human sources, for example through surveys, or extracted through interrogation. *Imagery Intelligence or IM.INT.* is data produced by electronic means that capture images, such as cameras. *Measurement And Signature Intelligence, or M.A.S.INT.*, is data produced mostly by technical means which are used to define the distinctive characteristics of a specific object. *Open Source Intelligence or O.S.INT.* is data collected through publicly available sources, such as newspapers, television, journals, and others. Finally, *Signals Intelligence or SIG.INT.* is data produced through the interception of signals or other mediums of communications between individuals or machinery.

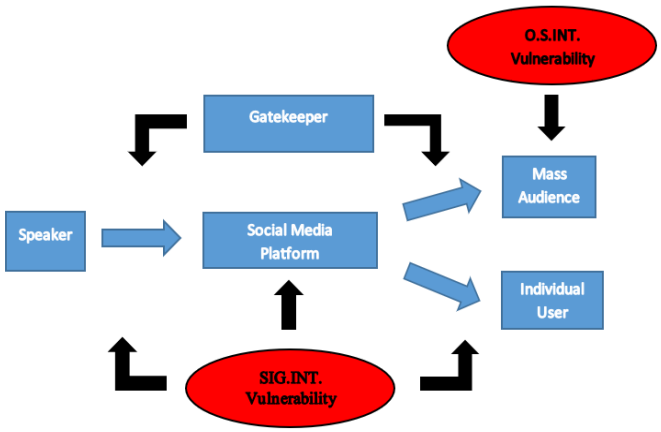
Through the above analysis of the Intelligence Cycle and the different categories of intelligence, it is possible to determine the way that social media are integrated into the cycle by intelligence agencies. Specifically, it becomes clear that social media can be used as intelligence sources, as they fall within

the *O.S.INT.* and *SIG.INT.* categories. Publicly available content which features descriptions or images of military vehicles, installations, troop movement and other similar data would be invaluable for an intelligence officer. On the other hand, a computer or other smart device infected by a malicious software which sends data to a third party involved in the conflict, unbeknownst to the user, could pose a serious threat of intelligence leakage in case the user exchanges information, that could be exploited by a seasoned intelligence officer, through a social media platform.

Having established the point of contact between the Intelligence Cycle and social media, it is possible to analyze the contact process and identify its vulnerabilities. The chosen analysis process is that of a simplified communication procedure, which includes the speaker (which could be either a private individual or content creator), the medium of transmittance (in this case the social media platform), the gatekeeper (the platform's moderators or AI moderating system) and the receiver (which could be either a private individual or the general public), in an amalgamation of the derivative models of the communication process proposed by Fougler (2004).

The flow of information begins from the speaker, who transmits information to the social media platform. The content passes through the platform, where the gatekeeper, or moderator, is able to review it, either before or after its transmittance, on to the receiver. In the communication process mentioned above, it is possible to identify three instances of point-to-point vulnerability regarding intelligence security: speaker-to-medium, medium-to-receiver (as a mass broadcast), medium-to-receiver (as a personal message). The above approach is considered as to the impartiality of both the platform and gatekeeper to either side of the conflict.

Figure 1: Social media communication process and intelligence vulnerabilities. Blue arrows represent the flow of information, while black arrows represent monitoring interference.



Source: own elaboration

The Intelligence Cycle is a process known to be used primarily by the U.S. Intelligence Community and NATO countries. However, for the semantic coherence of this research, it is necessary to establish that the opposite side does in fact use a similar method for intelligence acquisition. It is safe to assume that probably to some extent, Russian intelligence agencies use a similar methodology, which consists of at least three of the above steps; collection, analysis and dissemination. This assumption is made on the basis of these three steps being the minimum requirements for the production of a usable intelligence flow, as proposed by Smith and Brooks (2013). This theoretical reasoning is also confirmed by empirical data which show Russian operatives extracting data from content which is publicly available on social media, as shown in the subsection that follows.

Visualizing the Effects: Social Media in the Russo-Ukrainian Conflict

As a western world country, Ukraine has a significant number of social media users. According to the U.S. Agency for Global Media (2014), 50.9% of its overall population having access to household internet, and a total of 46% reporting using social media on a weekly basis, which is in accordance with the relative 93.4% global average. Since the beginning of the Russian *"Special Military Operation"* on February the 24th, 2022 (Polityuk & Mackenzie, 2022), there have been no reports of major connectivity shutdowns (NetBlocks, 2022), though there were some significant disruptions reported, especially in regions targeted by Russian strikes. It is therefore made clear that the overall availability of the internet and, subsequently, social media was and still is available to the majority of the Ukrainian population, despite the ongoing conflict.

During the conflict so far, there were several cases where Ukrainian civilians and military personnel published content on social media which included images of military operations and other relevant information. That content was then exploited by the Russian forces to strike at Ukrainian targets.

A notable example of this occurring was the targeting of a temporary military installation in Kiev. On the 20th of March, a Russian missile attack targeted Retroville Mall in Kiev, which was at the time reportedly used as a temporary storage and dispersion area for Ukrainian military equipment. The Ukrainian Security Service arrested a Ukrainian national due to the fact that he had publicly posted a video on a social media platform which featured military vehicles in the vicinity of the mall some time before the attack took place. This action was seen as providing intelligence to the Russian side and was justified by the Ukrainian Security Service as ultimately being the reason behind the missile strike (Duvnjak, 2022). The Ukrainian Security Service later released a video of the man admitting to and apologizing for his actions.

Should we exclude the possibility of individuals purposefully transmitting intelligence to the opposite side, it is made apparent that the uneducated use of social media, especially in the case of conflicts, constitutes a threat to national security, as it is also proposed by the U.S. Defense Technical Information Center (Nmah, 2007).

Problem Resolution: A Strategic Approach

Having analyzed the parameters and the significant effects of the problem, it is vital that an effort be made to remedy the issue. Taking into consideration the fact that from the moment the content is made available through social media, it is, in most cases, impossible to control whether it will be viewed and exploited by the opposing side, the best course of action for a state is to educate the populace on the aspect of *operations security*. Operations security, or OP.SEC. is defined as *"a systematic process by which a government, organization or individual can identify, control and protect generally unclassified information about an operation/activity and, thus deny or mitigate an adversary's/competitors ability to compromise or interrupt said operational activity"* (Michnowicz, 2006). However, in order for the process to be complete, it is necessary to educate both civilians and military personnel alike. Taking into consideration that military personnel, by definition, receives a basic OP.SEC. training, special attention should be given on the education of the civilian populace.

Another remediative approach would be to include the moderators of social media platforms into the OP.SEC. process. Through their ability to monitor the content made available on their platforms, either manually by the moderators or using AI technology, it could be possible to prevent intelligence compromisation. However, the involvement of a private, in most cases international, entity into a state matter, especially one as sensitive as national security, requires a special approach, which goes beyond the scope of this research. Furthermore, if any of the points of the communication process, especially the speaker and the platform, were infected by malicious software, a content monitoring process would still not be able to safeguard sensitive information. Despite this fact, it would be highly unlikely that the majority of the populace be infected with such a software without the competent authorities noticing.

Limitations and Further Research

There are several limitations to be taken into account regarding this paper. One of the main limitations is that, despite its theoretical justification, an important part of the reasoning process is based on empirical data and, therefore, requires further research to be completely established, as it is a multivariable topic. Another significant limitation was that due to the language barrier, it was not possible to use any Russian sources. A revisit of the topic, which will include Russian sources, might

provide further details on the part relating to the Russo-Ukrainian conflict. Furthermore, as of the completion of this paper, hostilities between the two parties have not yet ceased. It is possible that reviewing the topic after the completion of the conflict would provide further information and research material.

Conclusions

Taking the above reasoning into consideration, a number of conclusions could be summarized, regarding the topic in question. Firstly, empirical data portray that the Western and their corresponding Russian intelligence processes are similar in principle, as a result of the observed outcomes. Secondly, through the analysis of the social media communication process, it is evident that two types of intelligence vulnerabilities emerge, namely OS.INT. and SIG.INT. type vulnerabilities. Thirdly, in the case of conflict and in relatance to social media, the OP.SEC. process adheres to both civilians and military personnel, as both can compromise national intelligence security through the uneducated use of social media. Finally, in continuation to the previous point, it is in a nation's best interest to invest in the education of the general public on matters of OP.SEC., while a relevant remedial approach could also involve the institutions moderating the platforms' operations, though further research on the issue is necessary to reach any sustainable conclusions.

References

Chaffey, D. (2022). Global social media statistics research summary 2022. Smart Insights. Available at: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (Accessed: 25/07/2022).

Comunello, F., & Anzera, G. (2012). Will the revolution be tweeted? A conceptual framework for understanding the social media and the Arab Spring. *Islam and Christian - Muslim Relations*, 13 (4): 453-470.

Duvnjak, L. [@Luka_Duvnjak]. (2022). #Ukraine army arrested local resident of #Kiev Artemev Pavel Alexandrevich who recorded and posted a video on #TikTok where it was shown how Army of #Ukraine is using civilian #Retroville Mall as a place they fired artillery on Russian forces. [Video attached] [Tweet]. Twitter Available at: https://twitter.com/Luka_Duvnjak/status/1505975862310617089?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1505975862310617089%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.skai.gr%2Fnews%2Fworld%2Fvinteo-oukranou-prodose-ta-pyromaxika-sto-empor (Accessed: 25/07/2022).

Fougler, D. (2004). Models of the Communication Process. Davis.Fougle.Info. Available at: https://davis.foulger.info/research/unifiedModelOfCommunication.htm (Accessed: 25/07/2022).

Kaplan, A. & Haenlein, M. (2010). Users of the owrld, unite! The challenges and opportunities of Social Media. Business Horizons, 53: 59-68.

Michnowicz, R. (2006). OP.SEC. in the Information Age. [Masters dissertation, U.S. Army War College]. Defence Technical Information Center. Available at: https://apps.dtic.mil/sti/pdfs/ADA449260.pdf (Accessed: 25/07/2022).

NetBlocks (2022). Reports Archives. Available at: https://netblocks.org/reports (Accessed: 25/07/2022).

Nmah, O. (2007). The Effects of Social Media on National Security. [Masters disertation, U.S. Army Command and General Staff College]. Defence Technical Information Center. Ανάκτηση από Defence Technical Information Center. Available at: https://apps.dtic.mil/sti/pdfs/ADA449260.pdf (Accessed: 25/07/2022).

Phythian, M. (2013). Introduction - Beyond the Intelligence Cycle? In: M. Phythian (eds.). *Studies in Intelligence*. New York: Routledge, 1-4.

Polityuk, P. & Mackenzie, J. (2022). Ukraine rejects ultimatums as conflict intensifies. Reuters. Available at: https://www.reuters.com/world/europe/ukraine-refuses-surrender-mariupol-russia-warns-humanitarian-catastrophe-2022-03-21/ (Accessed: 25/07/2022).

Sacco, V. & Bossio, D. (2015). Using social media in the news reportage of War & Conflict: Opportunities and Challenges. *The Journal of Media Innovations*, 2 (1): 59-76.

Smith, C. & Brooks, D. (2013). Security Science. *Elsevier*: 177-198.

University of Michigan (2021). The evolution of social media: How did it began, and where could it go. University of Michigan Online Learning.Available at: https://sites.miamioh.edu/online-learning/2021/04/the-evolution-of-social-media-how-did-it-begin-and-where-could-it-go-next/ (Accessed: 25/07/2022).

U.S. Agency for Global Media (2014). Ukraine Research Brief. Broadcasting Board of Governors. Available at: https://www.usagm.gov/wp-content/media/2014/06/Ukraine-research-brief.pdf (Accessed: 25/07/2022).

Viekerk, B. & Maharaj, M. (2013). Social Media and Information Conflict. *International Journal of Communication*, 7: 1162-1184.

Zeitzoff, T. (2016). Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict. *Journal of Conflict Resolution*, 62 (1): 29-63.

Zeitzoff, T. (2017). How Social Media Is Changing Conflict. *Journal of Conflict Resolution*, 61 (9): 1970-1991.