The emergence of Big Drone Data?
Analyzing debates on drones as data gathering means in intelligence

Clemens Binder

oiip - Austrian Institute for International Affairs
clemens.binder@oiip.ac.at

Abstract

While their meaning for targeted killings in counter-terrorism operations has been emphasized, drones assume an important role in the rise of Big Data. By long-term surveillance, drones gather imagery on possible suspects, war zones and border regions. This data can be used by intelligence agencies in order to optimize operations, such as targeted killings. As during long-term surveillance, a great amount of data is gathered, drones add another dimension to the Big Data-nexus. This paper will investigate which debates revolve about the role that drones assume in the use of Big Data in intelligence by explaining shifts in the intelligence cycle that have been caused through Big Data.

***Keywords* –** drones, intelligence, big data, targeted killing, surveillance

1. Introduction

Hardly any other emerging military technology is as fiercely debated and attracts as much interest as drones, or Unmanned Aerial Vehicles (UAVs). Regardless if these devices are used for targeted killing or surveillance, debates revolve around ethics (e.g. Brunstetter/ Braun 2011, Finn/ Wright 2012) and legal implications. (Rosén 2014, Banks 2015, Boulanin 2015) UAVs are autonomous, armed or unarmed vehicles that operate via remote-control, in the case of military applications from thousands of miles away. Their deployment occurs for various reasons – most prominently however, drones are used for targeted killings in course of the "War on Terror". In this case though, discourse on the issue shapes a distorted image of reality. While targeted killings remain an important aspect of drone deployment, the Drone Data Program of the New America Foundation[1], a think-tank based in Washington, D.C., assesses that of 86 states with drone capabilities only 19 possess or are producing armed drones, leaving a great share of states with unarmed drones that are primarily used for surveillance aspects. Drone surveillance can happen domestically in order to establish border zone surveillance, for example in the Southern regions of the U.S. (Friedersdorf 2016), in order to survey war zones, for example in Eastern Ukraine (Tucker 2015) or to increase intelligence capabilities in disputed areas, such as the South China Sea. (Panda 2016)

Regardless if in the context of targeted killings or surveillance, drones share one central aspect - the acquiring of large amounts of data. Therefore, the question arises if drones lead to what Rothenberg (2015) defines as the *"emergence of Data-Driven warfare"*. Rothenberg sees drones as part of the growing data nexus and as supplementary devices in order to gather intelligence.

> *"The coordination of information gathered from drones lies not in what they can do on their own, but in their operation as part of a networked system that is complexly and multiply linked to other sources of data collection and analysis."* (Rothenberg 2015: 444)

As Rothenberg describes, data gathered by drones is especially used in the context of targeted killing, drones are capable of gathering data about suspects such as movements and create together with other forms of intelligence, especially Signals Intelligence (SIGINT)[2] a profile of the potential target in order to determine if an when a strike should be carried out. Drones produce a great amount of Imagery Intelligence (IMINT), data gathered by UAVs has assumed a central role in the military community.

[1] http://securitydata.newamerica.net/world-drones.html

[2] SIGINT describes intelligence such as communication and contacts via e.g. phone, e-mail

(Ackermann 2012, 2013) This paper will therefore explore the various ways drone data has influenced foreign and security policy by providing a new way of gathering intelligence data. This will comprise targeted killings as well as surveillance. It will be assessed which role drones assume in the wider Big Data-nexus and which advantages and challenges might arise for policy-makers by using UAVs for gathering data and intelligence. One notable mention should be made beforehand however, given the security implications drone data possesses, literature on this topic is scarce as are official documents as these are often classified and therefore not obtainable.

2. Research Question and Methodology

The difficulty given through the large amount of classified data puts restraints on the effective analysis of the role of drones in gathering data for intelligence. A limited amount of data does not allow a definitive response to the question of how drones are used as data-gathering instruments in intelligence operations. As drones as well as Big Data however represent fiercely debated topics and as Rothenberg's assessment proves, there is a strong connection between both of these issues. Therefore it is more plausible to investigate the debates that have evolved around drones within the Big Data-nexus and analyze how norms and perceptions of drones as data-gathering instruments have changed. According to this analysis, implications for policy-makers are likely to emerge.

The main question is therefore how drones influence norms and perceptions of gathering data for intelligence operations. Axelrod (1986: 1097) defines norms as follows.

> *"A norm exists in a given social setting to the extent that individuals usually act in a certain way and are often punished when seen not to be acting this way."*

For the question of how drones might have changed approaches towards data-gathering and the use of this data there arise two questions. First, are norms visible in discourses on the use of drones for gathering data, and second, how have norms changed through the use of drones.

The second important aspect in discourses are perceptions, or images. Images, as Herrmann et al. (1997) describe, influence choices in international politics by drawing images of relationships, creating perceptions of allies and foes and by creating strategic judgements on other actors. Given that UAVs are often used in conflict situations, images of non-state actors, allies and possible enemies or the fear of violation of sovereignty might draw policies that more strongly use drones as data-gathering instruments.

A discourse is, as described by Jørgensen and Philipps (2002: 1) *"a particular way of talking about and understanding the world (or an aspect of the world.)"* Analyzing a discourse means therefore investigating the factors that contribute to the understanding of topic of discourses, including language, structures and context. Hansen (2006: 33) describes security as a discourse, when issues are constructed as security concerns. However, Hansen distinguishes between collective and individualized security issues and assesses that this cleavage is constructed through political practices. This represents a development of the theory of securitization by Buzan et al. (1998), who perceive security issues as socially constructed, which also manifests in policies.

This paper will therefore not strictly investigate discourses, rather than debates, which include discourses and policies. Both dimensions should draw a comprehensive image of the understanding of drones as data-gathering instruments and how norms and perceptions are changing in this regard.

3. Defining Big Data and Intelligence

Big Data has emerged as one of the most important paradigm changes in the way data is perceived. Boyd/ Crawford (2012: 663) state *that "[t]he era of Big Data is underway."* What renders Big Data distinct to other phenomena of data collection is not only the sheer amount of data that is collected, but also how it is analyzed. Cukier and Mayer-Schoenberger (2013: 29) characterize this development as *"datafication"*, which means that various aspects[3] are being quantified by the use of Big Data. While companies have recognized the immense opportunities of Big Data for commerce and advertisement, its security implications are various. Before assessing how big data has shaped intelligence and security, it is however important to outline some general features of the phenomenon and big data analytics.

What is Big Data, after all? As Couch and Robins (2013:5) define, *"Big Data generally refers to datasets that are not susceptible to analysis by the relational database tools […] that have become familiar over the past twenty years […]"* Couch and Robins (ibid.) proceed to define characteristics of Big Data that comprise volume, variety, velocity and veracity. Volume describes the quantity of data, variety the complexity, velocity the speed of dissemination and change in datasets and veracity its reliability. Ulbricht and von Grafenstein (2016: 5) acknowledge that Big Data is a variety

[3] Examples in this case would be movements, contacts, interactions, particularly in context with social media platforms

of phenomena that affect a vast amount of social and political issue areas. In brief, Big Data therefore is defined in this paper as a set of data to which the prerequisites described above apply and that affects a political or social dimension. For this paper however, only the dimension of security and intelligence will be investigated.

In a military context, Big Data can change the approach and understanding of at least some aspects of warfare. The *"Weaponization of Big Data"* (Dunlap 2014: 110) enhances states capabilities in detecting suspects and develop profiles of contacts and movements of suspects by also adding facial images. Dunlap (ibid.: 109) describes this phenomenon as *"hyper-personalization of war."* Converging with Rothenberg's concept of "data-driven warfare", the impact of Big Data on security and intelligence policies is visible. Big Data in an intelligence framework combines various forms of intelligence, such as IMINT, SIGINT and in cases also human intelligence (HUMINT)[4] with the new forms of analytics, this convergence renders the creation of exact profiles of suspects possible. However, as will be described later on, this *"hyper-personalization of war"* is only one facet of the *"data-driven warfare"*. Before it is important to describe the concept of intelligence and to analyze the multiple intersections of Big Data and intelligence.

There is a wide range of definitions of intelligence among scholars and policy-makers alike, however, some basic notions are shared in a great amount of these. Starting with the definition of intelligence by Sherman Kent (1949: 3) who stated that *"Intelligence means knowledge"*, a variety of perspectives has emerged without delivering a clear definition. The basic notion that intelligence is some form of knowledge is amended by the definition of the organization that produces knowledge and which purpose the knowledge is produced for. These aspects can also be found in the Department of Defense's (DoD 2010) definition of intelligence.

> *"1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities."*

However, scholars assess that sufficient theorization in the field of intelligence studies has not taken place so far. (Scott/ Jackson 2004, Andrew 2004, Breakspear 2013, Marrin 2016) Especially the intersections between International Relations and Intelligence studies lack a more in-depth research, as intelligence is considered a major factor in international politics, yet, notable theories in IR such as realism and institutionalism tend to ignore its importance, also in regard of intelligence cooperation which, particularly in the Big Data-nexus represents an important policy field. Breakspear (2013: 692) pointed out the lack of a clear definition of intelligence and proposed one that proves suitable for this paper.

> *"Intelligence is 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."*

One concept central to the theoretical description of intelligence is the intelligence cycle, which describes four steps in intelligence – planning, collection, analysis and dissemination. (Phythian 2013: 1p.) The intelligence cycle delivers a framework for intelligence operations and the steps within the cycle determine central aspects for the intersection between Big Data and intelligence – especially in terms of data collection and data availability. As Hulnick (2006: 961p.) describes in his critique of the intelligence cycle, processes such as data collection and data analysis should run parallel instead of sequenced and coordination should be improved in order to detect gaps in data available for intelligence. The increasing availability of growing amounts of data could facilitate forecasting of events and accelerating the process, therefore Big Data poses an opportunity to ameliorate the intelligence cycle.

How does Big Data affect intelligence and where are its strategic implications for intelligence operations? Lim (2016: 634) describes three ways how Big Data interacts with the currently existing intelligence methodology. First, it assists in identifying developments, trends and anomalies, second, it generates hypotheses, and third, Big Data contributes in falsifying these same hypotheses. Applying these three factors to the intelligence cycle, Big Data influences all steps of the cycle, as planning is affected by the hypotheses generated and possibly falsified by Big Data, collection and analysis has to cope with rising amounts of data and is oriented on the identification of long-term developments, while the dissemination process could be amended by important observations, however could also suffer from an overflow of data. Does Big Data therefore improve the intelligence cycle? That is an assessment which is difficult to make. Big Data facilitates planning for the availability of data as well as the collection process, analysis and collection can easier run as parallel processes with the aid of great amounts of data. However, dissemination may suffer from the lack of analytical mechanisms and therefore from inaccuracy.

[4] HUMINT describes intelligence gathered through conversations, personal information and personal observation

Though its meaning for drones is currently rather low, the concept of Open Source Intelligence (OSINT) figures to be important in debates on Big Data and Intelligence. Defined by NATO (2001: 2p.) as follows

> *"OSINT is information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience [...] in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information and creates intelligence."*

OSINT is central in the debate on Big Data and intelligence, as openly available data increases the amount of data drastically, having positive and negative implications for intelligence. On the one hand, the variety of information OSINT offers drastically improves intelligence abilities, on the other hand, analytics grow more difficult in the light of the great amount of data. However, scholars (Hulnick 2002, Gibson 2004) agree that OSINT assumes an important role for intelligence. As the diffusion of commercially available drones grows, imagery recorded and shared deliberatively by users can be used as OSINT if required as well, making drones a likely future contributor to OSINT.

This chapter described the two main concepts surrounding the debate on drones and data-gathering. Big Data as emergent narrative in data sciences is of particular importance, as through increased data collection drones can facilitate analysis of data by providing imagery in a more flexible way than e.g. satellites do and in a more cost-effective way. Intelligence is one central field where drones and Big Data have especially emerged as shifts in discussions and policies. The following chapter will provide a perspective on the intersection between drones, Big Data and intelligence and give three crucial examples where IMINT through drones assumes an important role.

4. Drones and data-gathering

4.1. General perspective on drones, intelligence and data

Especially in military contexts, drones have developed into viable options as means for gathering data. Ackerman (2013) for example describes that the world has entered the "Age of Big Drone Data", where the analytics of drone data grows more crucial than the production of drones. Especially in the United States policymakers have adapted to the debate on analytics of drone data. As military personnel acknowledged that the Armed Forces are not able to efficiently analyze the great amounts of data gathered by drones (Ackerman 2012), the White House has announced to spend additional money on improving the Big Data analytics, including drone data. (Beckhusen 2012)

Within the framework of Intelligence, Surveillance and Reconnaissance (ISR), which has become a central concept of intelligence and security policy, drones are perceived as increasingly important instruments. ISR comprises three main aspects of clandestine operations, gathering data, observing areas and individuals of interest and recognizing possible abnormalities or other developments. Drones are perceived as the *"ultimate intelligence platform"* (Margolis 2013: 54), reports (Gertler 2012: 4) suggest that UAVs are primarily used as intelligence gathering instruments. The narrative of drones as intelligence-gatherers is continued by Lewis (2012) who states that the use of drones in gathering intelligence should minimize danger for human lives in order to collect HUMINT. However, as Pomerleau (2013) states, the lack of HUMINT and the heavy reliance on airborne intelligence has caused considerable challenges for U.S. military operations in areas such as Syria and Yemen. For gathering IMINT however, drones prove advantageous to satellite imagery due to their flexibility and disposability.

Abizaid and Brooks (2015: 19) outline an important aspect of the debates on drones by maintaining that the use of UAVs in ISR is not discussed controversially whereas critics on targeted killings are numerous. However, as described by Rothenberg (2015), the functions of drones as killing machines as well as data-gatherers are highly intertwined. Certainly, this debate could forge a stronger case for improving analytics of drone data in order to shape the discourse on drones primarily as intelligence-gathering instruments

4.2. Drones and targeted killing

Targeted killing remains the main task of drones in the perception of the wide public. Although, as stated in the introduction, states have acquired considerably higher amounts of unarmed UAVs, drone strikes, especially conducted by the U.S. have increased drastically. (McLeary, De Luce 2016) In the context of targeted killings, from a data science-perspective it is however more important how these so-called *"signature strikes"* (Rothenberg 2015: 450), strikes that are based on the analysis of gathered data, are conducted. These strikes differ from targeted killings as drones do not attack one predefined target, but observe the area of interest for an extended period of time, gathering data to facilitate the decisions on targeting and eventually conducting the strike. Signature strikes prove the clearest intersection between Big Data, intelligence and targeted killing as data is not collected specifically on one target but in order to detect targets, which represents a clear usage of Big Data analytics.

Another aspect that is exemplary for the connection between drone strikes and data gathering is the 'disposition matrix' the lists of targets for drone strikes from the U.S.

government. In this list, data, especially SIGINT is analyzed in order to detect suspects and categorize them as targets. (Zappalà 2015: 255) As Weber (2016: 108) describes, these databases render new data infrastructures and analytic mechanisms indispensable as kill-lists and databases emerge as central pieces of intelligence. UAVs in this regard can assume a two-fold role. On the one hand, targeted strikes are conducted based on the gathered and analyzed intelligence data that facilitate creating the databases. On the other hand though, drones, as describes in the context of signature strikes, can contribute actively in the set-up of these databases.

The perception of drones solely as killing machines does not prove true. A stronger awareness of the data-gathering capabilities could change the narrative of drones in order to effectively use them in counter-terrorism operations. Obviously, legal and ethical implications of targeted killings remain and require to be debated thoroughly, from a strict intelligence standpoint however, drones could prove viable instruments in counter-terrorism and counterinsurgency.

4.3. Drones and surveillance

As stated in the introduction, the majority of states that have acquired drone technology do not possess armed UAVs. That implies that a majority of UAV operations conducted are surveillance missions. Applications for drones in surveillance are numerous – domestic surveillance, border surveillance and the surveillance of conflict areas are a small sample of possible surveillance operations.

Particularly the deployment of drones in disputed areas is of importance. Two NATO reports by Nolin (2012) and Pintat (2014) highlight the importance of drones in ISR and gathering data by surveying conflict regions such as Afghanistan and Pakistan. As described by Gettinger et al. (2014: 6p.) drones can assist in distinguishing between civilians and combatants, and through extensive surveillance, can analyze insurgency networks. Drones can also provide surveillance capabilities in disputed areas where tensions are high, such as the South China Sea, where adjacent states have, according to New America, attempted to increase their respective drone capabilities. Particularly interesting is however the case in Eastern Ukraine, where secessionist forces use Russian drones in order to *"collect data to target missiles and artillery fire, which has proven to be an enormous advantage on the battlefield."* (Tucker 2015) This represents a case where non-state actors use drone data and intelligence in battle situations. According to New America, other non-state actors such as Hezbollah and the Islamic State have used drones for surveillance purposes as well, the use of drones by non-state actors in order to acquire intelligence is an important debate to lead.

Domestic deployment of drones consists primarily of border control and law enforcement operations. The U.S. has deployed drones to observe its Southern border, the EU-agency FRONTEX has also tested drones in order to improve European border control, an increase of drone surveillance of European border zones, especially maritime ones is currently debated. (Nielsen 2013, Csernatoni 2016) As Friedersdorf (2015) assesses, drones as means of border control, especially in the U.S. is not a subject of dispute, however, the domestic use of drones in order to police crime is. Wall/ Monahan (2011: 244) view drones as a central instrument in the War on Drugs, Stanley/ Crump (2011: 7p.) list a variety of domestic drone deployments by law enforcement agencies in the U.S. As law enforcements agencies also are considered a part of the intelligence network, risks, especially concerning privacy arise. Debates are led for example on persistent surveillance (McNeal 2014: 17) and on privacy infringements, which is why critique demands stronger regulation of gathering and handling drone data.

Both examples prove that drone surveillance is used in a variety of fields and possesses the opportunity for numerous applications. Especially in a domestic context however, surveillance and data protection evolve as crucial discussion points, in this regard, Big Data assumes a central role, constant surveillance would collect immense amount of data on every citizen which would prove dangerous if leaked.

4.4. Humanitarian aspects of drone data

Drone deployment for humanitarian reasons is an important, yet forgotten aspect of the technology. As already mentioned, drones can be used as means of surveillance in context of maritime border control, in this regard, drones could prove viable in the conduct of Search and Rescue (SAR) missions. However, for intelligence purposes, drone deployment for humanitarian reasons is interesting for other aspects. As Pintat (2014) describes, drones are *"excellent tools for collecting information in 'hostile' environments that have been struck by extreme weather conditions",* which have been contaminated or struck by other disasters. Information gathered by drones could be used in order to improve the planning of humanitarian actions.

Also in regard of possible human rights violations, the use of drones could prove viable. Sandvik and Lohne (2014) define the concept of the "humanitarian drone", drones that observe and act in conflict areas. As Sandvik and Lohne (2014: 159) describe, drones could *"win legitimacy for humanitarian interventions with shaky mandates, to shore* *up political support for R2P*[5] *missions, or to make UN 'peace enforcement' more effective."* Similarly, Whetham (2015: 207p.) proposes the deployment of surveillance drones in areas of suspected human rights violations, not only as means of surveillance, but also as means of deterrence.

The example of drone deployment for humanitarian reasons proves the versatility that drones offer for military and civil operations. As in other fields of deployment, Big Data plays an important role in humanitarian aspects as well, as collected data can offer information on areas struck by natural catastrophes or possible human rights violations.

5. Conclusion – drones, data, norms and images

In the beginning I stated that the general perception of drones is shaped by the public opinion on targeted strikes. Wall/ Monahan (2011: 243) also maintain that *"[b]y meshing aerial reconnaissance with aerial bombardment, drones function primarily as technologies of war."* Public discourse on UAVs therefore often ignores the important role of the technology in other fields, but especially undermines the perception of the data-gathering ability of drones. This is especially interesting regarding the images that exist of drones, as the difference between public discourse and the actual usage of drones is apparent. Different images of drones are drawn in different layers of the discourse. Drones and Big Data, albeit representing two technological developments which are linked closely to each other, rarely appear in the same discourses.

A different perspective however emerges when debating norms of data-gathering and how drones have shaped these norms. As in intelligence operations drones have clearly assumed important roles and figure to increase their significance for ISR, drones are generally accepted and even appreciated as data-gathering instruments. In context with targeted killings, signature strikes put a challenge to the development of norms concerning targeted killing and Big Data. Concepts such as "data-driven warfare" and the "hyper-personalization of war" certainly emerge as viable descriptions of the intersection between drone technology and Big Data. Regarding other issue areas described in the paper, drones however have integrated into the data-gathering nexus of intelligence operations.

While discourses on norms and images of drones clearly remain divided, the impact of drones on intelligence operations and security policy is quite visible. Drones offer an additional opportunity of gathering large amount of data and using this data for a diverse set of operations. To conclude, the possibilities of peaceful drone usage for intelligence operations needs to be emphasized and the technology could offer serious advantages in every step of the intelligence cycle.

Acknowledgements

I want to thank my former colleague Isabella Rebasso for assisting in research and preparation of this paper.

References

Ackerman, S. 2012 *Air Force Chief: It'll be years before we catch up on drone data*. Wired Online. <https://www.wired.com/2012/04/air-force-drone-data/> (Access 22.07.2015)

Ackerman, S. 2013. *Welcome to the Age of Big Drone Data*. Wired Online <https://www.wired.com/2013/04/drone-sensors-big-data/> (Access 22.07.2015)

Abizaid, J., Brooks, R. 2015. *Recommendations and Report of the Task Force on Us Drone Policy (Second Edition)*. Washington: Stimson

Andrew, C. 2004. *Intelligence, International Relations and 'Under-theorisation*'. Intelligence and National Security 19:2, 170-184

Axelrod, R. 1986. *An Evolutionary Approach to Norms*. The American Political Science Review 80:4, 1095-1111

Banks, W. 2015. *Regulating Drones: Are Targeted Killings by Drones Outside Traditional Battlefields Legal?* In Bergen, P., Rothenberg, D. (eds.) Drone Wars. Transforming Conflict, Law, and Policy. New York: Cambridge University Press. 129-159

Beckhusen, R. 2012. *White House Big Data Push means Big Bucks for Drone Brains*. Wired Online < https://www.wired.com/2012/03/big-data/> (Access 22.07.2015)

Boulanin, V. 2015. *Implementing Article 36 Weapon Reviews int the Light of Increasing Autonomy in Weapon Systems*. SIPRI Insights on Peace and Security 2015/1

Boyd, D., Crawford, K. 2012. *Critical Questions for Big Data*. Information, Communication & Society 15:5, 662-679

Breakspear, A. 2013. *A New Definition of Intelligence.* In: Intelligence and National Security 28:5, 678-693

Brunstetter, D., Braun, M. 2011. *The Implications of Drones on the Just War Tradition*. Ethics & International Affairs 25:3, 337-358

Buzan, B., Wæver, O., de Wilde, J. 1998. *Security. A new framework for Analysis*. Boulder: Rienner

[5] Responsibilty to Protect, a concept that allows humanitarian intervention in case citizens are endangered.

Couch, N., Robins, B. 2013, *Big Data for Defense and Security*. RUSI Occasional Paper 4

Csernatoni, R. 2016. *High-Tech Fortress Europe: FRONTEX and the Dronization of Border Management*. European Public Affairs

Cukier, K., Mayer-Schoenberger, V. 2013. *The Rise of Big Data. How it's changing the Way we think about the World*. Foreign Affairs 92:3, 28-40

DoD. 2010. *Dictionary of Military and Associated Terms.*

Dunlap Jr., C., 2014. *The Hyper-Personalization of War*. Georgetown Journal of International Affairs 15, 108-118

Finn, R, Wright, D., 2012. *Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications*. Computer Law and Security Review 28:2, 184-194

Friedersdorf, C. 2016. *The Rapid Rise of Federal Surveillance Drones Over America*. The Atlantic. <http://www.theatlantic.com/politics/archive/2016/03/the-rapid-rise-of-federal-surveillance-drones-over-america/473136/> (Access 25.07.2016)

Gertler, J. 2012. *U.S. Unmanned Aerial Systems*. Congressional Research Service.

Gettinger D. et al. 2014. *The Drone Primer. A Compendium of the Key Issues*. Center for the Study of the Drone, Bard College

Gibson, S. 2004. *Open source intelligence. An intelligence lifeline*. The RUSI Journal 149:1, 116-122

Hansen, L. 2006. *Security as Practice. Discourse Analyis and the Bosnian War*. New York: Routledge

Herrmann, R. et al. 1997. *Images in International Relations: An Experimental Test of Cognitive Schemata*. International Studies Quaterly 41, 403-433

Hulnick, A. 2002. *The Downside of Open Source Intelligence* International Journal of Intelligence and Counterintelligence 15:4, 565-579

Hulnick, A. 2006. *What's wrong with the Intelligence Cycle.* Intelligence and National Security 21:6, 959-979

Jørgensen, M., Philipps L. 2002. *Discouse Analysis as Theory and Method*. London: SAGE

Lewis, M. 2012. *Drones and the Boundaries of the Battlefield.* Texas International Law Journal 293

Lim, K. 2016. *Big Data and Strategic Intelligence*. Intelligence and National Security 31:4, 619-635

Margolis, G. 2013. *The Lack of HUMINT: A Recurring Intelligence Problem*. Global Security Studies 4:2, 43-60

Marrin, S. 2016. *Improving Intelligence Studies as an Academic Discipline*. Intelligence and National Security 31:2, 266-279

McLeary, P., de Luce D. 2016. *White House Drone Release Is Big on Numbers, Short on Detail*. Foreign Policy <http://foreignpolicy.com/2016/07/01/white-house-drone-release-is-big-on-numbers-short-on-detail/> (Acces 01.08.2015)

McNeal, G. 2014. *Drones and Aerial Surveillance*. Center for Technological Innovation at Brookings

NATO. 2001. *NATO Open Source Intelligence Handbook*

Nielsen, N. 2013. *EU looks to hybrid drones for legal shortcut on migration*. EU Observer

Nolin, P. 2012. *Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance*. NATO Parliamentary Assembly, Defence and Security Committee

Panda, A. 2016. *South China Sea: China's Surveillance Drones Make it to Woody Islan*d. The Diplomat. <http://thediplomat.com/2016/06/south-china-sea-chinas-surveillance-drones-make-it-to-woody-island/ > (Access 25.076.2016)

Phythian, M. 2013. *Introduction: beyond the Intelligence Cycle?* In: Phythian, M. ed. Understanding the Intelligence Cycle. New York: Routledge

Pintat, X. 2014. *Smart Defence: Platform Acquisition in the face of new technologies – Drones: A Case Study*. NATO Parliamentary Assembly, Defence and Security Committee

Pomerleau. M. 2015. *How technology has changed intelligence collection.* Defense Systems <https://defensesystems.com/articles/2015/04/22/technology-has-changed-intelligence-gathering.aspx> (Access 22.07.2015)

Rosén, F. 2014. *Extremely Stealthy and Incredibly Close: Drones, Control and Legal Responsibility*. Journal of Conflict & Security Law 19:1, 113-131

Rothenberg, D. 2015. *Drones and the Emergence of Data-Driven Warfare.* In Bergen, P., Rothenberg, D. (eds.) Drone Wars. Transforming Conflict, Law, and Policy. New York: Cambridge University Press. 441-462

Sandvik, K., Lohne, K. 2014. *The Rise of the Humanitarian Drone: Giving Content to an Emerging Concept*. Millenium: Journal of International Studies 43:1, 145-164

Stanley, J., Crump, C. 2011. *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*. American Civil Liberties Union

Scott, L., Jackson, P. 2004. *The Study of Intelligence in Theory and Practice*. Intelligence and National Security 19:2, 139-169

Tucker, P. 2015. *In Ukraine, Tomorrow's Drone War Is Alive Today*. Defense One <http://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/> (Access 25.07.2016)

Ulbricht, L., von Grafenstein, M. 2016. *Big Data: Big Power Shifts?* Internet Policy Review 5:1

Wall, T., Monahan, T. 2011. *Surveillance and violence from afar: The politics of drones and liminal security-scapes*. Theoretical Criminology 15:3, 239-254

Weber, J. 2016. *Keep adding. On kill lists, drone warfare and the politics of databases.* Society and Space 34:1, 107-125

Whetham, D. 2015. *Drones to Protect.* The International Journal of Human Rights 19:2, 199-210

Zappalà, G. 2015. *Killing by metadata: Europe and the surveillance-targeted killing nexus*. Global Affairs 1:3, 251-258