Digital Affordances and the Role of Open Source Intelligence (OSINT) Communities in Framing Contests

Steven Livingston, PhD
Professor, George Washington University;
Senior Fellow, Carr Center for Human Rights,
Harvard Kennedy School

Gregory Asmolov, PhD
Leverhulme Early Career Fellow
Russia Institute, King's College London

Abstract: Keck and Sikkink note that world politics at the end of the twentieth century involved nonstate actors that "interact with each other, with states, and with international organizations as networks. Transnational advocacy networks frame events and issues in such a way as to alter the behavior of states. Soft power in this way can overcome the advantages of material power. Our goal in this paper is to situate these same dynamics in a 21st century digital information environment. Information exchange in transnational advocacy now involves the use of various digital technologies, including earth observation satellites and digital networks. This alteration in information and service exchange also introduces new types of non-state actors, including commercial technology firms, technology consultancies, and Open Source Investigations (OSINT) -- volunteer communities that use digital affordance and Big Data to investigate events and processes. We explore three OSINT volunteer communities – UK-based *Bellingcat*, Russia-based *Conflict Intelligence Team* (CIT) and Ukraine-based *Informnapalm*. By way of in-depth interviews with key members of these OSNIT communities and a review of existing literature, we seek to provide a more nuanced understanding of contemporary issue framing practices in digital environments. The paper proposes an alternative vision of the framing activation processes, one best characterized as a contest between rival networked "framing coalitions," which rely on different digital affordances and connective action (Bennett and Segerberg, 2013).

> All we have to do is to hang a bell about the Cat's neck. When we hear the bell ringing we will know immediately that our enemy is coming. . . . An old Mouse arose and said: "I will say that the plan of the young Mouse is very good. But let me ask one question: Who will bell the Cat?"
>
> Aesop's Fables

Introduction:

The battle of wits played out between perfidious cats and vulnerable mice serves as a colorful metaphor for considering high-stakes power dynamics in the 21st century. To avoid the cat, mice must be alerted to its presence. Yet who will *bell* the cat? In recent years, some part of the answer has been provided by commercial information and communication technologies -- from billions of multifunction mobile phones to earth observation satellites and social media platforms. By using various digital technologies, nonstate actors collect evidence and call attention to significant events and trends that would go otherwise undetected. The aptly-named Bellingcat, an open-source investigative collective, offers one example. Founded in July 2014 by British blogger Eliot Higgins, it marshals the online sleuthing skills of numerous investigators to ferret out threats. Open source investigations are, says Higgins, "not just about one photograph, or one video, it's about *the network of information that exists and exploring that network online*" (Sullivan, 2017. Emphasis added). Similarly, the Atlantic Council's Digital Forensic Research Laboratory (DFRLab), refers to its investigators as "digital Sherlocks," researchers who use open-source data to investigate war crimes and counter suspected disinformation campaigns (Czuperski, et al., 2015).

Bellingcat's investigation of the destruction of Malaysian Air flight 17 in July 2014 illustrates the idea. Based on photos and videos found online, Bellingcat concluded the plane was shot down by a Russian Buk surface to air missile.

> When that missile launcher was travelling through Ukraine, we had photographs shared online, people discussing the photographs, people tweeting about it. It created ripples, and what we try to do is identify them, and understand them in the context of all the other material. That gives us a very solid case (Sullivan, 2017).

Whereas Bellingcat's conclusions were generally supported by official investigations and news accounts in the West, an alternative narrative emerged from Russian official accounts and investigators – doppelgängers to their Western counterparts. For example, a group of anonymous Russian bloggers calling themselves the "Anti-Fake citizen journalists group," issued a 44-page report offering what it said was the truth about the downing of MH-17(Anti-Fake, 2016). The document, published in English, was released two weeks before the publication of the findings of the official, Dutch-led criminal investigation of the incident. According to the "Anti-Fake" report, Ukrainian forces were responsible for the downing of the civilian aircraft. This was also the position of the Russian government. The Dutch Joint Investigation Team found that the Buk missile involved in shooting down the aircraft had been transported from Russia on the day of the crash and fired from a location under the control of pro-Russian rebels. The mobile launching platform was then returned to Russian territory following the incident. Yet according to "Anti-Fake," Bellingcat is biased against Russia, misinformed, and traffics in fabricated evidence. According to Bellingcat and most Western observers the Anti-Fake group is dealing in disinformation.

What is going on here?

In response to the use of advanced digital technologies and open-source data by nonstate actors, accused states have begun using information and

communication technologies in an effort to *undermine* war crimes and human rights investigations (Hoffman, 2007, p. 14). They do so by clouding investigations with a dizzying array of claims and counterclaims, falsified evidence, and ad hominem attacks on individual investigators. Disinformation campaigns might even be understood as a part of a new kind of warfare that is known by several names: Nonlinear or hybrid warfare, New Generation War (NGW), or simply the Gerasimov doctrine, named after Russian military chief of staff Valery Gerasimov. As a warfighting doctrine, it represents a shift from a heavy reliance on kinetic force to a complex interplay among a broad spectrum of warfare modalities, from thermonuclear war to information operations (Perry, 2015). Information operations include the "collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent" (Rand, 2018).

This paper offers a conceptual framework for thinking about *one* of the possible reactions offered by states accused of war crimes and human rights abuses. On some occasions, the reaction is restorative of human rights norms. States that have fallen out of compliance with broadly shared norms come to acknowledge their mistakes and even embrace international human rights norms. This is the finding of much of the research associated with the boomerang and spiral models of transnational advocacy (Keck and Sikkink, 1998; Risse, Ropp, and Sikkink, 1999, 2013). Yet perpetrator responses to accusations also include more repression and violence directed at human rights workers, journalists, and civil society organizations. These are real or physical, material forms of resistance to accusations of abusive practices by repressive states. Our interests are more precise. We focus on the way accused states pushback in digital space. This

typically involves the use of disinformation, or what might be more appropriate to refer to it as *networked framing contestation*.

A key concept in our approach is "network framing," which can be thought of as the shaping of an issue and narrative as the result of a complex interplay of human and algorithmic factors in digital space. While speaking of "network framing" or "network framing contests" is a bit cumbersome, it helps scholars avoid taking implicit political positions, as is the case with references to "disinformation." While some cases are intuitively obvious, scholars ought to avoid embracing a position regarding the factual accuracy of a given narrative or the intention of its authors. As critics of "disinformation" research often note, western political institutions have also been known to prevaricate on such matters of war and peace (Bennett, Lawrence, and Livingston, 2007; Robinson, 2016).

In this paper, we explore new opportunities for framing and counter-framing, and the emergence of new actors that harness technological capabilities to promote frames. Following a review of relevant theoretical constructs, the paper explores three networked framing communities that conduct open-source intelligence around the conflicts in Ukraine and Syria: Bellingcat, Informnapalm, and the Conflict Intelligence Team. We turn first to a review of framing theory.

Framing in conflicts:

Framing theory has a long and venerable career as a core concept in several disciplines, including anthropology (Bateson, 1972), behavioral economics (Tversky and Kahneman, 1981), sociology (Goffman, 1974), political communication (Entman,

1993), social movement studies (Snow and Benford, 1988), and transnational advocacy research (Keck and Sikkink, 1998). What do we mean by framing?

According to Entman, framing involves "selecting a few aspects of a perceived reality and connecting them together in a narrative that promotes a particular interpretation" (Entman, 2010, p. 391). What Entman calls *substantive* frames perform at least two of the following functions:

1. Defines effects or conditions as worthy of a response
2. Specify a causal interpretation of a problematic condition
3. Convey moral judgment
4. Endorse remedies or improvements intended to address the problem

Not all social conditions, no matter how injurious, are accorded the status of a problem, or something worthy of a response. The emerge of a problem reflects power dynamics as much as it does the characteristics of underlying condition. Put another way, there is no essential correlation between demonstrable harm and problem status. The link between cancer and heart disease, for example, was contested for decades, as is now the link between burning fossil fuels and climate change, at least it is for some (Oreskes and Conway, 2010). Racial and gender discrimination is rejected by some as a problem, despite what many see as the obvious harm both cause, while others regard voting fraud in the United States as a serious problem, despite the absence of evidence of its actual widespread existence in the United States. The first point of contestation, therefore, is problem status.

Should an issue rise to the status of a recognized problem, attributing responsibility for its cause is the next step in the substantive framing process. If gun violence, for example, is understood as a problem, what are its causes? Is it found

in the easy availability of guns? Or is it instead the result of mental illness or the influence of violent music videos and videogames, as the National Rifle Association claims? Moral attributions and solutions to a problem flow from the logic and associations embedded in an embraced causal attribution. If poverty is accepted as a problem, a particular causal attribution points to particular moral conclusions and solutions. If, for example, poverty is understood as the consequence of individual character defects, negative sanctions directed against the poor are called for (limited unemployment benefits, minimal welfare benefits). If poverty is instead understood as an inevitable outcome of global capitalism, a system characterized by fluid capital but relatively fixed labor, the unemployed person's character is not called into question (though the morality of the economic system is), and training programs and even guaranteed basis income schemes are given support. In short, how a social condition is framed privileges some solutions over others (Edelman, 1985).

In case of conflict, framing is also concerned with attribution of responsibility for particular incidents and the causes of the conflict in general. The focus on incidents and the larger conflict is also related to moral judgments of different sides of the conflicts and considerations as to how it should be resolved. Framing of conflict participant (combatant and non-combatant alike) applies to both specific forces on the ground (e.g. local groups and regional state actors) and to global powers that are thought to be associated with the conflict. And because the same issues arise around different incidents in the same conflict, one can expect to see meta-frames emerging repeatedly in various conflict-related incidents over time. In other words, each new incident is not framed anew with fresh angles, but more likely according to established narratives.

Most germane to this paper, however, are questions about the nature of political power in framing contests. If we hold in mind that frame dominance is as much a reflection of political power as it is about the nature of underlying conditions, understanding power dynamics have added significance. In a digitally networked environment, how are frames created, by whom, and contested how? Entman's cascade activation model argues that framing capacity is distributed unevenly (2003), with elite officials occupying privileged places at the top of a framing cascade. He describes a stepped hierarchy of framing capability, with the White House at the top of the hierarchy and the public at the bottom, and with various intermediate players between them.

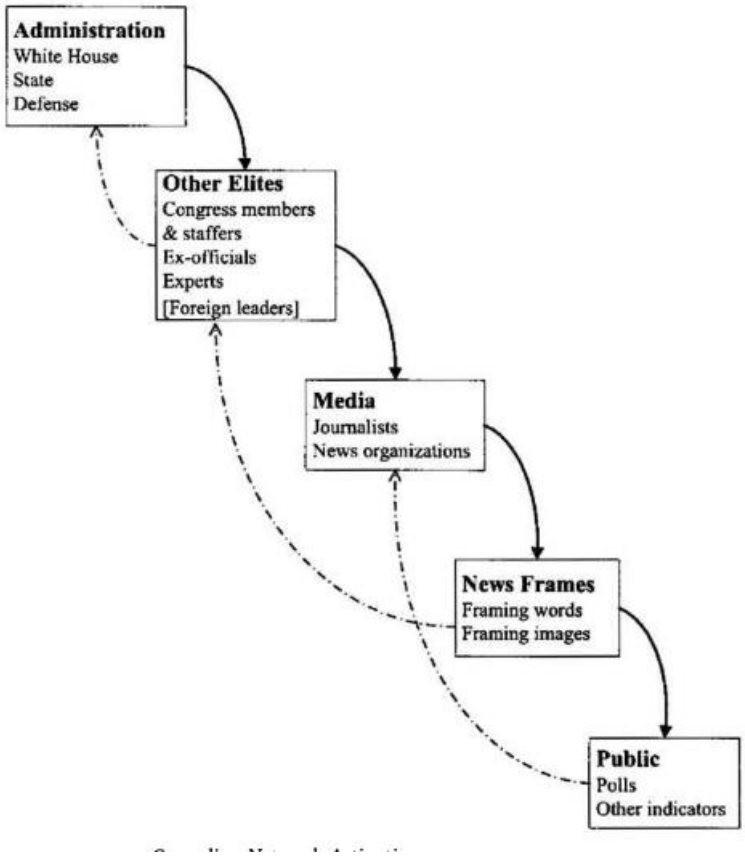

Figure 1: Cascade Activation Model
Source: Entman, *Projections of Power*

In most of the cases, framing contests are dominated by the actors on the top of the cascade (p. 418). Counter framing – offering countervailing evidence and reasoning -- requires large scale mobilization of media and counter-elites, something that occurs only rarely according to Entman's original model. The minimal capacity of the public to offer counterframes to those offered by dominant elites is visually represented by the dashed lines working their way up the left side of the diagram in figure one. Also, public framing is mediated by formal news organizations, the destination of the weak arrow headed back toward, but never quite reaching elites. The metaphor of cascading waterfall highlights that "ideas activate and spread from one location on the network to others" but the direction of transmission, in most cases, is from the top to the bottom, while "spreading ideas higher, from lower levels to upper, requires extra energy—a pumping mechanism" (Entman, 2003, p. 420). Therefore, "Public opinion is typically a dependent variable, although it sometimes feeds back to influence elites" (p. 420).

Entman's model was formulated in a mass media era defined by a limited number of media outlets that shaped the contours of a one-to-many media content distribution model. A television station (one) broadcast its signal to a mass audience (many). Today, communication is best defined as many-to-many. At least theoretically, anyone came communicate with everyone on a digital network. As a result of the partial shift from one-to-many communication system to a many-to-many system, Entman's original cascade activation model fails to take into consideration what Castell's calls "counterpower," the idea that social media platforms enable publics to push back against elite frames (Castells, 2013). The development of information communication technologies, perhaps especially digital networks, leads us to question Entman's pessimistic assessment of the role of publics and their

limited capacity for meaningful participation in framing contests. These limitations are particularly visible when the dynamics and the structure of framing contests are taken from a specific national political context to the level of international conflicts that include a diversity of institutional actors, non-governments organizations, groups of activists and various publics, all now linked (with firewalls and other forms of censorship factored in as limitations in some instances) together.

Meraz and Papacharissi (2013) offer a reconsideration of the role of publics in framing contestation by introducing the notion of "networked framing." Rather than passive recipients of frames originating at the top of a cascade, publics in digitally networked space enjoy considerable framing agency. Meraz and Papacharissi define networked framing as a "process through which a particular problem definition, casual interpretation, moral evaluation and/or treatment recommendation attain prominence through crowdsourcing practices" (p.159). In such a formulation, Entman's "public" is conceived of a "crowd" organized on or by a digital platform. Crowdsourcing in this way has its own framing agency, though the cascade metaphor breaks down as a result. One might instead think of a framing maelstrom, with a core swirl of contesting claims and counterclaims, with little eddies off to the side where "filter bubbles" reside in perhaps obdurate indifference to countervailing ideas of any kind (Pariser, 2011). Twitter hashtags and retweeting offer another example. If enough users – human and bot – favor a tweet, its prominence increases. It is said to be trending. *Network framing allow a temporally and geographically dispersed crowd to elevate the prominence of specific frames associated with an issue (as captured in a tweet or meme) that might otherwise go unrecognized by traditional institutional gatekeepers*. The recent #metoo movement hashtag, for example, raised awareness and produced significant effects regarding

sexual harassment at the workplace and in other social settings, even in the face of initial indifference and stonewalling by various powerful individuals and institutions. Contrary to earlier frame activation models, Meraz and Papacharissi found that "analysis of prominent actors and frames highlighted the fluid, iterative processes inherent in networked framing as frames were persistently revised, rearticulated, and redispersed by both crowd and elite" (p.138).

While the notion of "networked framing" challenges the traditional understanding of the public as a mostly passive participant in framing contestation, it also has a number of limitations. First, it addresses a crowd as an unspecified group that include journalists, activists, bots, and ordinary users. While it replaces the notion of a relatively passive public lacking agency with the notion of an active crowd, it does not tell us much about the nature of the new actors that take part in frame activation. No doubt, there are many variations in crowd morphology. Parsing them is made more challenging by the proliferation of sock poppets, botnets, and trolls, all mimicking a disinterested but perhaps alarmed person who just happens to engage with an issue online. We turn to these considerations next with a review of a limited number of public entities qua crowdsourcing communities.

New Framing Actors

The notion of "networked framing" invites attention to new types of "framing agents," humans and semiautonomous technologies that are involved in digital networks like Twitter and Facebook. This includes four groups of actors: 1. human, 2. non-human, 3. pseudo-human, and 4. non-authentic actors. The first group is obvious but complex. The group of non-human actors presented by algorithms that

influence the visibility of a particular segment of information within flows of information that rely on various platforms and the results of search engines. Also, bits of computer code designed to amplify information online can be thought of as pseudo-human actors. Bots that create networks for participation in DDoS attack intended to block content can also be thought of as either non-human or pseudo-human actors. (AI is narrowing the essential distinctions between these two categories.) Trolls and bots that are managed by human users relying on fake identities (sockpuppets) in order to manipulate online discourse and proliferate information can be considered non-authentic actors. The latter can be considered as manifestation of "computational propaganda", that is defined as "**"**the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion" (Wooley and Howard, 2016, p. 4886).

Earlier framing contestation models regarded frame dominance in a mainstream or elite press (The New York Times and Washington Post in the U.S.) as the core objective. Besides cascade activation, W. Lance Bennett's Indexing model focused attention of frame dominance in elite media content. Framing in an earlier era involved common characteristic of coverage of events and actors in a limited number of news outlets. In the tsunami of information in the digital era, just getting heard above the din is the first hurdle. Attention becomes the core objective. Various digital affordances are harnessed to address this challenge. Put simply, where information overload on digital platforms is a problem, *the ability to amplify a targeted message becomes a key attribute of power*.

In this way, framing agents rely on digital affordances that create opportunities for data collection, analysis and proliferation (Gibson, 1977). Norman (1988), defined affordances as the "fundamental properties that determine just how the thing could

possibly be used" (p. 19). Bucher and Helmond (2017) approach digital platforms "as a set of affordances <…> that enable and constrain human action." In that light, "social media platforms constitute a form of environment too, composed of pathways and features in their own right" (Bucher & Helmond, p. 18).

Affordances can also be linked to the availability of new type of data sets that can be used in network framing contests. Although data are generated from a growing array of sources, a few examples come to mind. Information is generated by both human and non-human sensors that are connected to a common network. Conflict-related data may include user generated content (including photo and video that shared from mobile devices), CCTV cameras, and geospatial data generated by satellites and UAVs. Data are also generated by hacktivists that move restricted information into public domain. Finally, data are generated by traditional actors, including news media, NGOs, and state actors. Conflict related big data might also include various types of open data sets, including official documents, statistical data that is provided by governments, and the conclusions of academic research.

An additional set of information that is generated by different electronic devices is meta-data – the data about data that allow observers to track the location and timing signatures. Location and time stamps of photos and video taken by smartphones or geolocation-equipped cameras offer an example of meta-data. Conflict related data and meta data offer new opportunities for activation of frames. Open source data about the conflict are valuable to those who are interested in understanding the it and countering the frames of particular events and issues that are promoted by others. Harnessing open source data and meta data and using it to its greatest potential requires skills and collaboration among different actors. The fact that data are now available is only a part of the story of digital network framing

contestation. We turn next to a description of the entities – also often occupying only digital space – that make use of data and meta-data in their efforts to frame broader understanding of events and processes.

OSINT

Open Source Intelligence (OSINT) is defined as information "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[1] That said, the analysis of new information environment may suggest a need for reconsideration of what is included in OSINT. Data and meta data that can be found on open networks includes GEOINT (satellite and aerial photography), SIGINT (data about communication between participants of warfare including voice messages), and TECHINT (specific information about weapons and equipment used by armed forces). Moreover, the outcomes of hacktivist activities that are shared online can be thought of as a part of Cyber Intelligence (CYBINT). Each of these areas were once controlled by state intelligence agencies. Today, they are, to varying degrees, available to civilians.

As highlighted by Groll (2015) “the greater availability of open source intelligence has been enabled in part by enormous growth in the commercial satellite industry.” Some of the companies hire former intelligence experts in order to conduct open source analysis. Groll concludes that “the explosion of open source information on Russian moves in Syria speaks to the changes the American intelligence community is being forced to reckon with, to both consider information posted on

[1] As defined in Sec. 931 of Public Law 109-163, entitled, "National Defense Authorization Act for Fiscal Year 2006."

social media and a greater public awareness about geopolitical developments." Jeffrey White, a former Defense Intelligence Agency expert, remarked, "We used to send reconnaissance units out to hilltops and report back on hostile forces. Now you've got people running around taking pictures and posting them."

In other words, various digital affordances contribute to changes in what is considered as "inaccessible and restricted," which increases the potential value of OSINT. That includes user generated data from social media, satellite imagery and imagery that is generated by UAV's, as well as additional sets of data and meta-data. The analysis of data and meta data generated around conflicts requires advanced data mining technologies. It also requires experts who are able to use these technologies in order to analyze information, and generate data visualizations of various sorts that make the information more accessible to mass audiences.

As argued by Groll (2015), "From commercial satellite photos to Facebook posts, tracking Russia's military intervention in Syria has never been easier for the world's amateur and professional spies." According to Toller (2015), in case of Ukraine, OSINT relies both on new actors and new digital platforms:

> Grassroots projects and individual bloggers attempt to cut through government narratives on both sides to provide at least a glimpse of the situation as it is. Their work usually amounts to collecting photographic and video evidence of battles and military equipment in eastern Ukraine, geolocating, and crowdsourcing the verification efforts to provide greater context for the collected data.

Toller highlights that both groups and individuals use blogs and social media accounts to conduct online investigations. At the same time, different platforms offer

open-source data about the conflict. That includes online mapping platforms e.g. *LiveUAMap* (http://liveuamap.com) that aggregate and geolocate reports about the Ukrainian crisis, as well as *Lostarmour.info* project that aggregate data about Ukrainian ammunition that was either captured or destroyed as a part of conflict.

While the way these groups work may recall the practices of OSINT experts in traditional militaries, these groups emerged as online networks of digital volunteers who are unaffiliated with any security organization. Digital affordances generate more data about conflict, more opportunities to collect and analyze data, and to reach and amplify conclusions. Technology allows unaffiliated OSINT networks to produce intelligence information relying on analysis of open-source data and meta data in order to present a data-based narrative about a conflict. In short, *OSINT-enabled actors represent a form of the public that assumes a robust and meaningful counter-framing position in a framing contestation*. We explore digital network framing contestation using OSINT in the remainder of the paper.

Methodology

This paper focuses on the OSINT digital networks that investigate conflicts. As a case study, we look into groups that collect, analyze and distribute information related to conflicts in Syria and Ukraine, specifically concerning Russian involvement in these conflicts. Our cases include three groups that can be regarded as networks of experts that use OSINT to collect information about conflicts. At the time of this writing, our research has included interviews in London, Moscow, and Kiev of all of the key individuals in the three OSINT organizations reviewed here.

Bellingcat was founded in 2014 by British blogger and citizen journalist Eliot Higgins. According to Bellingcat.com website: “Bellingcat uses open source and social media investigation to investigate a variety of subjects, from Mexican drug lords to conflicts being fought across the world.”[2] The second group is the Russia-based *Conflict Intelligence Team* (CIT) that was founded by Ruslan Leviev, also in 2014. Relying on OSINT, CIT conducts investigations of conflicts in Ukraine and Syria. The third group is *InformNapalm*. Coming in reaction to the Russian invasion of Crimea, it was founded in March 2014 by military expert Irakli Komaxidze from Georgia and journalist Roman Burko from Ukraine. Defining itself as an “International volunteer community,” according to the InformNapalm website, the community “mostly relies on open sources and widely employs different OSINT methods of information gathering.”

We explore four major themes:

1. What digital affordances are relied on by the organization?
2. How is collaboration structured? What is the division of roles between participants in OSINT groups?
3. What are the major objects of framing?
4. What is the response of the traditional state-affiliated actors to the activities of OSINT groups?

In order to respond to these questions, we rely on a mix of qualitative and quantitative methods. The interviews were focused on the methods and practices used by OSINT networks, the structure of collaboration between these networks and other actors, and the response of state-affiliated actors to their activities. We also

[2] https://www.bellingcat.com/about/

conducted a quantitative content analysis of the publications found on their respective websites. We review our findings in the next section.

Modes of Collaboration and Objects of framing.

Bellingcat

Bellingcat's launch by British blogger and citizen journalist Elliott Higgins on July 15, 2014 was made possible by donations raised on the Kickstarter crowdfunding platform. Higgins notes, "Bellingcat.com will unite citizen investigative journalists to use open source information to report on issues that are being ignored." Prior to Bellingcat, Higgins blogged under the "Brown Moses" moniker about online video and images of weapons and ammunitions that were used by all sides of the Syrian conflict. Higgins how to identify illegal weapons, including cluster bombs and chemical munitions, and trace their origins. One of the first significant cases was the chemical attack on Ghouta, Syria on 21 August 2013. In his open-source analysis, Higgins was able to link the sarin attacks to President Bashar al-Assad's forces.

Bellingcat, said Higgins, has two major goals. First, he wants to unite "a group of citizen investigative journalists who through using open source information have transformed journalism and solidified themselves as experts in their fields." Second, he wants to focus on learning and developing new open source tools for data analysis. Higgins concluded, "It's important to note these investigations were done by a variety of people, showing the importance of making open source investigation tools and techniques available to anyone. This is what Bellingcat is about." Higgins has also said he is interested in building "a network of people who know open-source investigation techniques [so] we can start spreading these ideas to more and more

people." In another interview he declared that the ultimate purpose of Bellingcat was to strike fear into war criminals and human rights abusers. "I want the very idea of open-source information existing to put the fear of God into the sort of people who have something to hide, because they'll know there's a network of people primed to use it to expose what they're trying to keep hidden" (Massie, 2015)[3]

Bellingcat relies on harnessing collective intelligence of the open community of experts from various fields. In some cases, the members of Bellingcat are called "citizen investigative journalists." For instance, according to Mashable.com, Bellingcat is, "A group of citizen journalists armed with simple intuition and an Internet connection have been collecting information more nimbly than American spies."[4] However, it also has been addressed as "investigative search network**"** or "a network of citizen-spies" that brings together open source and social media investigation experts. Bellingcat members have also been characterized as a small army of "armchair intelligence analysts (who) are debunking propaganda and uncovering war crimes without ever leaving home" and "venturing into territory occupied by government intelligence agencies by virtually investigating conflict zones where access is nearly impossible" (Schatz, 2016).[5]

In order to engage a broad community of potential experts in analysis of video and images, Bellingcat used open-source tools, including Storyful, which is itself a commoditized network. Founded in Dublin in 2010, Storyful analysts attempt to verify videos and stories found on social media. With offices in Hong Kong, Ireland, and

[3] Watch out for Bellingcat By Christopher Massie, CJR JANUARY 12, 2015 https://www.cjr.org/business_of_news/bellingcat_brown_moses.php
[4] http://mashable.com/2014/07/23/citizen-journalists-mh17-spies/
[5] Schatz B., January/February 2016, These Digital Sleuths Are Sticking It to ISIS and the Kremlin http://www.motherjones.com/politics/2016/02/bellingcat-intelligence-analysts-ukraine-russia-isis/

New York, Storyful looks at three major points of verification for social media content: date, location and the identity of the person who posted. In analyzing video, the type of weather and visible landmarks seen in a video. But Bellingcat also relies on digital volunteer networks assembled on its Twitter feed and website. This open approach allows collaboration with unbounded community of potential contributors that have knowledge and expertise in different areas.

Higgins also started using Slack chat-tool in order to collaborate around investigation of the downing of the Malaysia Airlines Flight 17 in Eastern Ukraine. Some of photo-sharing websites and Google Earth are also used to determine the specific location on the photos from the war zones. In addition to geolocation, the analysis is concerned with authentication of images as well as interpretation of specific details that can be found on the photos.

Bellincat's investigation of MH-17 caught the attention of pro-Kremlin forces. Contrary to the Kremlin's official narrative that put the blame on Ukrainian forces, Bellingcat concluded Russian forces, in collaboration with pro-Russian Ukrainian rebels, were responsible for the tragedy. Finding the exact position of the BUK launcher and its movements became a focus of attention in the OSINT investigation. In this effort, Bellingcat collaborated with the Russia-based Conflict Intelligence Team (CIT), another open-source investigatory initiative. Higgins also joined the Atlantic Council, a Washington-based think tank, as a senior fellow associated with its Digital Forensics Research Lab (DFRLab). DFRLab tracks the activities of both the Russian and American governments. For instance, it investigated arrival and deployment of American-made lethal weapons in Ukraine, based on information that was published by the "Azov Battalion," formerly volunteer based Ukrainian combat

unit that was integrated within Ukrainian National Guard.[6] This information was distributed by pro-Russian government media, including the TV Channel Zvezda, an outlet of the Russian Ministry of Defense, and the state sponsored news agency RIA-Novosty[7].

Bellingcat and the Atlantic Council produced a report "Hiding in Plain Site," which documented Russian presence and operations in Eastern Ukraine, despite Russian claims that its military is not involved in this conflict. HBO and Vice News, in collaboration with the Atlantic Council, and by extension Bellingcat, produced "Selfie Soldiers," a documentary that traced the movements of a Russian soldier according to photos (with meta-data) posted to his Russian social media account.

The outcomes of Bellingcat investigations challenged the narrative that were promoted by Russian government. Moreover, the contribution of Bellingcat to the official investigation of the MH-17 tragedy threatened Russian major global interests. The analysis by Bellingcat became a major part of information war. It not only suggested alternative interpretations of major events that took a part in Syria and Ukraine, it also debunked Russian disinformation by exposing forged evidence created by the Russian government. While some pro-Russian bloggers and online experts looked for Bellingcat mistakes, others focused on Higgins by questioning his objectivity, credentials, and motives. Internet ses, a Wikipedia page about Higgins was vandalized by Internet trolls. And RT, the state-sponsored Russian news network, ran segments that attacked his credibility, in part by lifting quotations out of context. Higgin's Brown Moses blog was also accused of working for a range of

[6] American Lethal Weapons Could Already Be on the Ukrainian Front Line https://medium.com/dfrlab/american-lethal-weapons-could-already-be-on-the-ukrainian-front-line-9dc6fd98630d

[7] https://tvzvezda.ru/news/vstrane_i_mire/content/201801110910-v9nf.htm and https://ria.ru/world/20180111/1512402445.html

security service, including the C.I.A., Mossad, and M.I. 6. Some experts also accused Higgins of manipulating satellite data about MH17.[8] But ridicule was the most common form of attack. Figure 2 is a cartoon published in various Russian media. It suggests that Higgins follows the order of NATO leadership in in an effort to conceal their own responsibility for attack against civil populations and to blame Russia.

Headline: American Center Atlantic Council hired the founder of Bellingcat for publication of critical essays about Russia:
General: We slightly destroyed local village
Higgins: I got it. I am going to draw Russian tanks in Ukraine.
Figure 2

Still, Bellingcat forced those who were target for open-source investigations to change their online behavior. For instance, Russian soldiers were ordered to avoid selfies and to hide meta-data that would disclose information about their location. According to Higgins, Jihadists from Islamic state also started "telling each other not to film stuff and to be careful about what you have in the background."[9]

[8] Bidder B., Bellingcat Report Doesn't Prove Anything', Spiegel Online**,** June 04, 2015
[9] Schatz B., January/February 2016 Issue, These Digital Sleuths Are Sticking It to ISIS and the Kremlin, http://www.motherjones.com/politics/2016/02/bellingcat-intelligence-analysts-ukraine-russia-isis/

Conflict Intelligence Team

Conflict Intelligence Team (CIT) was founded by Russian activist and blogger Ruslan Leviev in 2014. Born in Surgut in Western Siberia, Leviev became interested in computer programming and hacking while still in school. After moving to Moscow a few years before, his first experience with political activism came in December 2011 when he took part in a protest against results of the Duma elections. He was arrested and held by police for two days, an experience that deepened his commitment to political activism. In 2012, he began assisting Russian opposition leader Alexey Navalny with various online projects, including efforts to bypass the state-sponsored blocking of Navalny's website. Leviev also founded an independent online broadcasting company called Newcaster TV used to broadcast oppositional events.

Fortuitously as it turns out, Leviev's also has an interest in aviation, a hobby that ended up playing a role in his efforts to monitor the Maidan Square protests in Kiev in February 2014. As Ukrainian special police forces were shooting on crowd on Maidan Square, Leviev was listening to the conversations of air traffic controllers in Kiev's airport. As the fighting escalated, he followed and tweeted about the rapidly escalating number of departing private jets carrying senior Ukrainian politicians out of the capital. A number of online flight-tracking applications, including Flightracker, also helped Leviev and others conduct open source continuous mapping of the flights and offer an account of the movement of key figures at this crucial moment in Ukrainian history.

A few months later, with war in East Ukrainian in full swing, Leviev also began monitoring images of pro-Russian rebels in Eastern Ukraine in an effort to determine the origins of their weapons and ordinance. In May 2014, he also created a Telegram chat for those who were interested in investigation of open sources data about conflict in Ukraine. Telegram is a secure, encrypted messaging application. Among those following Leviev's posts were volunteers from Bellingcat. The major topic of investigation was the presence of Russian soldiers in rebel-controlled Donbass area of eastern Ukraine. After one of the pro-Russian rebels was captured by Ukrainian forces, Leviev found his account on "Odnoklassniki" (Classmates), a Russian social network. The captured soldier's wife then confirmed his identity as a Russian soldier named Aleksei Generalov. In September 2014, Leviev decided to follow Bellingcat model and used LiveJournal blogosphere to open a blog called "War in Ukraine."

In May 2015 Leviev and his team used information from Russian social network Vkontakte to confirm that three soldiers from a Russian special forces intelligence unit were killed in Eastern Ukrainian. The team analyzed metadata of the photos from the soldiers' profile to show that they were present in Eastern Ukraine.[10] Leviev and his team also used fake identities to contact relatives of the soldiers via social networks. In this way they confirmed their names and the location of their graves. Members of War in Ukraine team then used local contacts to take pictures of the graves. The results of the investigation were distributed by a number of Russian liberal media websites and the Western media. Later, a number of dedicated websites were also created to crowdsource information about Russian soldiers who

[10] Websites as http://fotoforensic.com are used in order to extract all metadata from a particular image.

were killed or captures in Eastern Ukraine.[11] Russian president Vladimir Putin soon declared that information about army and security service casualties was a state secret. At about this time, the Conflict Intelligence Team was created. As Leviev describes it, he and other investigators started working as a team around May-June 2014.

> By that point many of us had been doing what's now called OSINT (Open Source INTelligence). By summer 2014, the sheer volume of information to analyze and process became so large that we had to gather a team to distribute tasks and work more efficiently. It is then when a call to make a team was issued and several people replied. At that point we were but IT and social network specialists able to conduct complicated multi-criteria searches across big data.

Leviev noted that the conflict in Ukraine offered an especially productive information environment for open-source analysis because of the high volume of user-generated data. The military combatants and the local population were robust users of social networks, in part because of the availability of broadband connectivity. Local cultural practices also facilitated data collection. Dashboard cameras in cars in Russia and Ukraine are common, in part because a video record of events can help a motorist avoid insurance scam.

According Leviev, investigating Russian activities in Syria was more challenging, in part because of the relative paucity of online content. The team followed the methodology of their counterparts from Bellingcat and analysed user-

[11] That included LostIvan.ru portal (now deactivated) and http://gruz200.net/.

generated video from Syria and satellite imagery. For instance, in one of the cases, based on geolocation analysis, they challenged the arguments of Russian military that the target of Russian attacks were territories under ISIS control and demonstrated that the territory was actually controlled by other groups that opposed Bashar Assad. They also challenged Russian official statements about lack of causalities among civilian populations.

Leviev highlighted that the investigations are not his "personal achievement but a joint labor" of CIT team, that relies on "IT and social network specialists able to conduct complicated multi-criteria searches across big data."[12] Like Bellingcat, CIT also used crowdfunding in order to support its activities. Leviev also emphasizes that CIT does not consider itself to be a citizen journalism group, in part because it relies on methods most journalists would "deemed unethical."[13] Leviev's team developed special techniques in order to engage people in data collection and analysis, as well as investigated online behavioral patterns of Internet users in order to identify the best strategies to obtain available information[14]. In interview to *Foreign Policy*, Leviev argued that his activities are closer to what combatants do than it is to journalism. CIT also works anonymously. Leviev is almost the only member of group who is known to the public.

The CIT is often accused of data manipulation and forgery, though most of these accusations come from Russian or Assad pro-government groups and media outlets. One pro-Russian website published a photo-shopped screenshot of Leviev's e-mail and Facebook message exchange with other oppositional activist. According

[12] Ruslan Leviev About our Conflict Intelligence Team (CIT) and our investigations, 07.09.2015 https://citeam.org/about-our-team/
[13] https://citeam.org/about-our-team/
[14] For additional analysis of ethical aspect of OSINT analysis see: Toller, A. (2015). Dying in Secret: The Ethics of Investigating Russia's Ukraine Casualties, Global Voices Online, https://globalvoices.org/2015/05/26/russia-ukraine-soldiers-death-investigation/

to the fabricated screenshot, Leviev askes to be forgiven for publishing fake information as part of a CIT investigation into a chemical weapons attack in Syria. Screenshots of a fake blog post were also used to accuse Leviev of developing a computer ransomware to extort donates to CIT.

Russian state media dedicated special attention to Leviev. A popular television anchor, Vladimir Soloviev, called Leviev “a spy” and ask FSB to “take care of him.” Russian television news stories also claim that Leviev hacked the accounts of Russian soldiers and their relatives to obtain information about their participation in conflicts in Ukraine and Syria. Russian governmental media also describes Leviev as an agent of the West who works for CIA and is sponsored by George Soros, the billionaire financier and supporter of liberal causes. He also has been accused of being a collaborator of terrorists and jihadists in Syria. His former collaboration with leading oppositional activist Alexey Navalny is used to argue that his investigations are politically motivated. Yet according to Leviev, so as to avoid giving them publicity, larger media outlets like “Russia Today” and those that are linked to Russian Ministry of Defense tend to ignore CIT. And when it is mentioned, it is often referred as the “Ukrainian group,” which ignores the fact that CIT is based in Moscow and has no direct ties with Ukraine.

Leviev has also been summoned to the military prosecutor’s office to explain CIT’s investigations of Russian causalities in Ukraine and Syria. Publishing these data, it was said, constituted treason. Members of Leviev’s family and his landlord were also summoned to the offices of the security services. CIT members are also targeted by Russian hacker groups, including CyberBercut, a pro-Russian hacktivist group. Hackers were able to hack one of Leviev’s personal e-mail accounts and his Livejournal blog. He has also been “doxed.” Hackers published Leviev’s passport

number and his telephone phone number and home address. After the doxing incident, hackers used images said to be stolen from his account to portray him as a rapist and paedophile and that he supports groups that harm animals. These claims, Leviev says, are untrue.

InformNapalm

Ukrainian journalist Roman Burko and Georgian military expert Irakli Komaxidze launched InformNapalm following the Russian invasion of Crimea in March 2014. Burko, who at the time of the invasion was living in Crimea, began documenting the presence of Russian soldiers, including a Russian army attacks on Ukrainian military bases. Burko says his purpose at the time was to reveal the identity of the "green men," a reference to the green masks worn by Russian soldiers to hide their faces. Irakli Komaxidze soon joined Burko to analyze the images.

According to InformNapalm website, its purpose is "to inform the world about the real role of the Russian government in ongoing hybrid conflicts in Ukraine, Georgia, other countries of Eastern and Central Europe, and in the Middle East." The topics that are covered include identification of Russian soldiers engaged in the conflicts. By looking for photographs online and in news accounts, InformNapalm even tried to identify Russian pilots. According to Burko, any pilot who know his name might become known will reconsider actions that might result in civilian deaths. Russian official media have since started concealing the faces of pilots.

InformNapalm now includes approximately thirty volunteers from over ten countries who analyze and verify data, conduct research, translate documents and design content displays. The volunteers communicate through dedicated chats on

Facebook, as well as on secure Telegram and Signal messengers. The founders of the project highlight that investigations rely mostly on “open sources and widely employ (and) different OSINT methods of information gathering.” This includes data from other volunteer organizations, including those using UAVs that are able to provide footage from conflict zones.

While InformNapalm team emphasizes that it does not encourage hacking, they have received information in this way. According to InformNapalm, “any information obtained from hacktivists undergoes a thorough verification based on alternative sources.” In some cases, InformNapalm crowdsources the analysis of high-volume leaks. According to Burko, unlike media organizations, InformNapalm is interested in publishing secrets of its perceived adversaries in an effort to cause financial losses and damage operational capabilities. InformNapalm members consider themselves as participants in the conflict and Ukrainian loyalists.

Content Analysis: mapping the issues of framing.

This section presents preliminary results of content analysis of the blogs of two OSINT communities – Conflict Intelligence Team and InformNapalm[15]. The analysis sought to identify dominant frames found in OSINT communities. The analysis covered 313 items. The dataset is divided between content devoted to the conflicts in Ukraine and Syria.

[15] The results of the analysis are subject to additional consideration in order to confirm inter-coder reliability.

Conflict Intelligence Team (N=80)

	Attribution of Responsibility	Involvement	Casualties	Weapons	Anti-fake	Other
Ukraine	1	4	5	0	2	6
Syria	19	8	16	12	4	3
Total	20	12	21	12	6	9

InformNapalm (N=233)

	Attribution of Responsibility	Involvement	Casualties	Weapons	Anti-fake	Other
Ukraine (139)	19	79	1	9	7	28
Syria (93)	25	36	2	9	5	14
Total	44	115	3	18	12	42

A preliminary content analysis of blogs by OSINT communities allows us to identify four major types of conflict-related issues that can be considered as object of framing. These include:

- Attribution of responsibility for specific incidents as a part of conflict (e.g. downing of MH-17 flight in Eastern Ukraine or attribution for targeting civic population in Syria)
- The scale and the type of Russian military involvement in Ukraine and in Syria (e.g. if Russian soldiers present in Ukraine territory)
- The scale of casualties among Russian soldiers in Ukraine and Syria
- The type of weapons and ammunitions used by Russia and/or their allies in conflicts (e.g. cluster bombs or chemical weapons).

In addition, a substantial number of posts are concerned with the analysis of allegedly fake posts by pro-Russian sources.

This simple comparison between CIT and InformNapalm content allows us to identify a noteworthy difference between the two groups. CIT is particularly concerned with investigation of causalities among Russian soldiers that took part in both conflicts. That is a topic of more than 25% of their posts. However, this issue is largely ignored by the Ukrainian project. At the same time, almost 50% of the posts by InformNapalm are concerned with proving Russian involvement in military operation in Ukraine and Syria. That can be considered as an indicator for the difference in motivation of two groups as well as in their appeal to different target audience. CIT addresses Russian domestic audience in order to raise attention to the loss of Russian lives far from home and to question the legitimacy of sending soldiers to conflicts beyond Russian borders. InformNapalm addresses mostly the international audience in order to demonstrate the scale of Russian involvement in the conflicts.

This basic and preliminary content analysis might be regarded as an invitation to more detailed investigations of differences in the motivations of digitally enabled framing actors. While InformNapalm portray themselves as digital soldiers that take a part in the battle on the Ukrainian side, CIT members highlight that they are activists that seek to hold their government accountable. At the same time, apparently, relying on the discussion above, Bellingcat seems to be mostly driven by international humanitarian norms.

Discussion

The main purpose of this paper is to consider how new digital affordances affect framing theory. We focused on the new actors that have emerge as a part of framing contest around conflicts in Ukraine and Syria, and specifically Russian role

within these conflicts. The focus on the groups of OSINT volunteers allows us to examine the process of counter-framing activation, and specifically the role of digital affordance in a context of framing contest, the structure of collaboration between various actors that participate in framing relying on digital affordances, the object of framing and the response of traditional state actors to emergence of new agents of framing.

First, OSINT online initiatives allow us to identify the digital affordances that contribute to the emergence of new actors involved in framing and counter-framing activities. We can identify several. User-generated data, such as social media feeds, commercial satellite imagery, and video produced by dashboard cameras or by drones contribute to the creation of an information ecology supportive of OSINT. Other features include services such as Flightracker. Online communication, though usually secure from surveillance by nonstate actors (state surveillance is another matter) can still be intercepted by hackers. The capacity to move restricted data into a public domain relies on programming and hacking affordances.

A second set of affordances deal with data and meta-data analytics. This includes dedicated tools for data analysis, such as fotoforensic.com, findexif.com or izitru.com that analyze image meta-data. Other digital mapping platforms assist with analysis of the geolocation of an image. Bounded networks of experts (epistemic communities) and unbounded networks of crowds also participate in analyses. The latter can be conceptualized as crowdsourcing affordances. Crowdsourcing affordances include crowdfunding – the mobilization of the financial resources of the crowd to support data collection, data analysis and amplification. The analysis also includes verification affordances relying on information from bounded networks of

experts, as well as dedicated tools that seek to find members of the crowd who are familiar with a specific region, situation, or have other background knowledge.

A third set of affordances deal with distribution and amplification of reports and analyses. That includes data visualization. Storyful offers one example of an organization dedicated to this affordance. Another would be The Engine Room, a New York based technology consultancy that assists in data management and visualization. The proliferation affordances also includes non-human actors (e.g. bots) in order to support data amplification.

We can also see how affordances are interconnected, with data collection, analysis, and amplification affordances relying on collaboration and crowdsourcing affordances. Various forms of participation of crowd, experts, bounded group of volunteers and other actors in data collection, data analysis, and data amplification can be summed up as connective and networking affordances that support digitally mediated collective and connective action (Bennett and Segerberg, 2013). Collaboration can also take place without disclosing the identity of some of the participants. Anonymity in hostile environments is essential. In this respect, we can also conceptualize certain affordances that ensure security and anonymity of actors – such as Telegraph, Signal, and other encrypted communication platforms.

We have discussed how digital affordances give rise to new actors – both human and algorithmic -- who take part in frame contestation. The cases of OSINT community highlight that framing activated not by a single actor, but relying on coalitions that include a variety of actors. For instance, the analysis of leaks from Russian authorities that proved Russian involvement in Ukraine was possible due to collaboration of hackitivists, OSINT volunteers, general members of digital crowds that take a part in crowdsourcing and traditional media organizations. The digital

affordances that support connective action allow to connect between actors with different resources and different skills (e.g. data collection, data analysis, development of content and content proliferation) around common object, which is participation in activation of counter-frames. The key actors in these networked coalitions, however, are neither citizen journalists, nor traditional organizational actors (though DFRLab and Storyful might be considered as such). These are networks of people with a variety of typically non-materialistic motivations that come together due to new opportunities to collect, analyse and amplify data about situations that concern them. One would say they are principled actors.

The proliferation of *state-sponsored* framing initiatives, on the other hand, relies on the collaboration of different sort but somewhat similar actors that also develop coalitions around common objects of framing. This includes pro-government hackers (some of whom are paid, such as is the case with the so-called troll factory in St. Petersburg), and state-sponsored media. State-sponsored framing networks might also include international journalists and academics, as well as trolls and bots who amplify the visibility of information that is supportive of a particular frame or, alternatively, fuel the profile of a counter-frame. Amplification also comes from conspiracy websites and YouTube channels like “InfoWars.” In 2017, journalists discovered that InfoWars had republished over 1,000 RT news stories without permission or alteration. Copyright infringement issues aside, the U.S.-based InfoWars amplified RT’s frames, which are in turn often in alignment with the Russian news agency Sputnik and the themes found in the broader Russian framing network online. This are characteristics of network framing that is activated relying on collaboration between a variety of actors, and rely on digital affordances.

While all the sides of framing contest harness digital affordances and activate framing via construction of networked coalitions, the analysis of OSINT volunteers group sand their relationship with state-sponsored actors highlight what apparently seem to be some substantial differences in the objects of framing. The traditional objects of framing deal with specific events and issues. The content analysis indetified a number of these issues including attribution of blame for specific attacks, the scale of Russian involvement and casualties in Ukraine and Syria, as well as the type of ammunition that is used as a part of this conflict.

All four types of events deal with a general conflict-related framing issues as identified by Entman. According to Entman, framing contestation involves competing interpretations concerning the ontology of a condition and its causes. Is smoking, burning fossil fuels, poverty, discrimination a problem? If so, what causes it? While moral attributions accompany causal attributions, the scope of the framing competition is usually contained. In addition, since these objects of framing are repeatedly addressed by OSINT volunteers over a long period of time, they can be considered as elements of strategic counter-narratives that deal with the Russian role in conflicts in Ukraine and Syria, and more generally Russian role in Post-Soviet space, the Middle East and the global international system.

That said, the interviews with the key figures in OSINT communities highlight that state's response to promotion of alternatives frames by OSINT volunteers has a different nature. While there are some state-sponsored activities that conform to traditional modes of issue-framing, most of their efforts are dedicated to a different object of framing – not the issues, but the actors that take a part in framing contest. This includes undermining the legitimacy of opposing institutions, throwing doubt onto the credibility of their analysis, or their claims to expertise, and the integrity of

their motivations. Members of Bellingcat, CIT and InformNapalm describe efforts to discredit them and question their patriotism and legitimacy. They are often characterized as shills of foreign intelligence agencies or villainized persons like George Soros. The publication of personal information seeks to spoil their reputations and sometimes threaten their lives. In all these cases, we can see that the major object of state-sponsored framing is the members of OSINT volunteer communities and more generally the members of networked coalitions that take a part in activation of counter-frames.

The investigation of state's response to emergence of new framing actors, however, allows to identify an additional set of objects as a part of framing contestation. When the contest around framing of issues and efforts to undermine the legitimacy of new framing agents are not sufficient in order to protect state's control over conflict related frame activation, there is one forms of response that seeks to restore the balance of power which has been disrupted by OSINT communities and their collaborators. One can argue that trolls that disrupt online discussions and bots that amplify narratives are focused on an even bigger fish: the global information system itself. Understood in this way, disinformation is not a matter of putting more or less emphasis on some aspect of a knowable reality. Instead, it seeks to undermine rational discourse and the weight of brute facts. Bennett and Livingston (2017) argue that disinformation campaigns play on and deepen the cynicism that feeds the delegitimation of legacy liberal institutions, including the press. They often weave bizarre interpretations of actual events into a series of reoccurring conspiratorial narratives that confound more than they clarify. The goal is to undermine facts altogether, creating a phantasmagorical world of confused public resignation. A deliberate increase of uncertainty that convince

audiences that no source, no institution can be trusted. It intends to lay waste to Enlightenment principles: the weight of facts and rationality existing separately from brute political power, the rule of law, and the recognition of rights. It also seeks to trigger feeling of apathy and indifference among broad audiences.

To sum up, the analysis allows to differentiate between three types of framing objects that rely on connective action and supported by a variety of digital affordances. First is an issue-focused framing, when the rival sides of framing contest activate frames with alternative interpretations of specific issues, that are often grounded in different strategic narratives. The case studies, however, illustrates how the members of OSINT communities themselves became an object of framing for state-sponsored actors. In that way *"issue-framing"* by members of OSINT communities is addressed by *"actor-framing"* activities by state-sponsored networked coalitions of actors. The further, analysis, however identifies a third object of as a part of framing contestation, which is about not issue or actors, but the environment where the contest takes place. This object is the global system of information circulation.

The analysis of the objects of framing allows to explore the response of traditional state actors to emergence of new agents of framing and highlight the asymmetric nature of framing contest. While the issue-focused framing is associated with disruptive actors that rely on digital affordance and challenge state sponsored frames, the coalitions of state-affiliated actors seek to restore balance of power by focusing on the new rival framing agents and on global information system as objects of framing contest.

We suggest to conceptualize this asymmetric response of state-affiliated actors to OSINT volunteer communities and their collaborators as a manifestation of

"sustaining power". Sustaining power is the ability to undermine the counter power of digitally enabled non-state actors. This term given to a combination of traditional forms of coercion (prison, torture, murder) of those who challenge repressive states to sophisticated digital responses that seek to undermine the legitimacy and credibility of critics and the information system. In that case, application of sustaining power as a part of framing contests is directed predominantly not toward issues, but toward the actors and the global system of information circulation.

Conclusion

The aim of this paper was to explore the process of framing activation in a context of framing contest related to Russian involvement in conflicts in Ukraine and Syria. It addressed this goal through focus on new actors that take a part in framing activation relying on digital affordances. The analysis of cases that deal with new "agents of framing"- the communities of OSINT volunteers, allows to argue that framing activation is an outcome of networked collaboration between a variety of actors, that constitute "framing coalitions" around common objects of framing. In that way, framing can be considered as participatory practices, while the nature of the engagement goes far beyond participation in information sharing (as highlighted in the notion of networked framing by Meraz and Papacharissi). The analysis illustrates that framing contest relies on digitally mediated mobilization of a variety of resources offered by different actors that include resources for data collection (if in legal or illegal ways), data analysis, development of content and content proliferation, as well as mobilization of social capital, financial resources and knowledge of Internet users.

In that light, framing activation can be considered as a form of connective action of a number of different actors (framing coalitions) that rely on digital affordances.

The analysis also allows to review the structure of framing activation. Unlike the metaphor of cascade that has been introduced by Entman, the contest of networked coalitions underline lack of any hierarchy or specific structure around activation of frames. The collaborative networked nature of activation of frames presents a complex reality of horizontal relationships between a diversity of actors that contribute their resources, when the object of framing offers a common denominator that triggers emergence of specific network, that deals with framing of specific issue. While sharing objects of framing, the volunteering actors may have substantially different motivations as illustrated by comparison of CIS, BellingCat and InformNapalm.

The challenge that is created by counter-framing as networked mobilization of the resources of a variety of actors, is addressed by state-sponsored actors in a few ways. First, state-sponsored actors also harness new digital affordances and seek to activate the frames relying on networked mobilization of a variety of actors. Though, the nature of participation in state-sponsored framing coalitions may substantially differ and include relying on paid incentives, non-genuine actors and vertical coordination. However, that might be not sufficient in order to address the power of new actors in framing contestation. The state-sponsored shift in objects of framing illustrates the asymmetric nature of state's response and can be considered as manifestation of "sustaining power" that aims to mitigate the effects of digital innovation on framing contests and restores the balance of power that has been challenged by new actors on the framing battlefield.