Strategic Communications and Social Media in the Russia Ukraine Conflict

by
Elina Lange-Ionatamishvili
and
Sanda Svetoka

Chapter 12 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Elina Lange-Ionatamishvili and Sanda Svetoka of the NATO Strategic Communications Centre of Excellence in Latvia, in Chapter 12, discuss the role of social media in this conflict. In the Internet era, the battle for hearts and minds has never been more important. Social media is a trust-based network that provides fertile soil for intelligence collection, propaganda dissemination, and psychological operations (PSYOPS) to influence public opinion – or to lead adversaries into harm's way. 'Soft' cyber attacks can be as severe as any attack on critical infrastructure. In Ukraine, they have generated fear, uncertainty, and doubt about the economic, cultural, and national security of Ukraine, while promoting positive messages about Russia's role in Crimea and eastern Ukraine. The authors provide recommendations for defence against such attacks, including how to identify them, challenge them, and how to develop a resilient political narrative to withstand false propaganda.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Strategic Communications and Social Media in the Russia Ukraine Conflict

Elina Lange-Ionatamishvili
Sanda Svetoka
NATO Strategic Communications Centre of Excellence

1 Introduction

The new information environment has changed the nature of warfare. The events in south-east Ukraine have demonstrated that a conflict can be won without firing a single shot and some of the key battles can take place in the cyber and communications domains rather than on the land, air and sea. As Thomas Elkjer Nissen said in his recent book, the internet, cyberspace, and social media can be used to collect intelligence or even to target people and organisations. Such tactics may be employed in isolation, but they are much more likely to be an integral part of a larger strategy.[1]

> *Key battles can take place in the cyber and communications domains rather than on the land, air and sea.*

The operation for the take-over of Crimea was a particularly bold example of an influence operation where the traditional role of conventional forces was mini-

1 Thomas Elkjer Nissen. *#TheWeaponizationOfSocialMedia. @Characteristics_of_ Contemporary_Conflicts*. Copenhagen: Royal Danish Defence College, 2015.

mised. As the conflict continues to develop in the east of Ukraine, Russia continues to exploit the opportunities offered by new technologies and the new information environment. It does so with the purpose of influencing the hearts and minds of its audiences: if Russia succeeds in mobilising its supporters, demonising its enemy, demoralising its enemy's government and armed forces, and legitimising its own actions, then really there is no need for conventional fighting in order to subdue Ukraine.

In the modern-day operations cyberspace plays an increasingly important role. A targeted attack by an adversary in the cyber environment is often understood as an attack on the computerised systems which help us run our daily lives and businesses, sustain critical infrastructure and conduct financial transactions amongst other things. As the former White House advisor Richard Clarke writes, a cyber-attack can mean that these vital systems go down and we see exploding oil refineries, derailing trains, runaway satellites, food shortages, and much more.[2] But what we do not often realise is that we can be attacked in the cyber environment by an adversary presenting manipulative information to us with the intent to affect our perception of the situation and our decision-making, and provoke some resulting action. The real-life consequences of this 'soft' cyber-attack can be as severe as an attack on a critical infrastructure.

2 Strategic Communications and Cyberspace

Strategic Communications (StratCom) is a mind-set which implies placing communications at the heart of a strategy. It means that our activity is narrative-driven and we communicate it to different audiences through coordinated words, images and deeds. Cyberspace plays an increasingly important role in StratCom as our dependency on modern technologies, computer networks and the internet grows day by day. We use it for receiving and conveying information, for coordinating our actions and also for analysing the environment around us in order to detect and evaluate potential threats.

Cyberspace is often used in a conflict in order to take out the communications systems of an adversary. However, the conflict in Ukraine has demonstrated that cyberspace can also play a role in conducting a narrative-driven operation where the main targets are not the machines or networks but the minds of the people.

The internet and social media, due to their ability to multiply information at high speed and at little cost, are increasingly used for propaganda, information warfare, and influence operations, all of which can tangibly change both the perception and behaviour of the target audience. It is a highly dynamic, user-driven, constantly changing environment where it is easy to get a message to 'go viral', and also difficult

2 Richard A. Clarke and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2011.

to track the initial source of information, verify its authenticity, and separate fact from fiction.

With the increasing popularity of social media platforms, the concept of social cyber attack is gaining traction.[3] It allows for a low-cost, speedy way of manipulating society's perceptions in order to cause disruptive behaviour in real life. The social cyber attacks observed during the crisis in Ukraine led to an assumption that at least part of them were implemented in an organised way, as part of a larger influence strategy.

3 Psychological Operations (PSYOPS) and Social Media

Psychological Operations (PSYOPS) is a military activity which is aimed at influencing the perceptions, attitudes and behaviours of target populations. The perception is usually affected by either emotional appeals or rational arguments, corresponding to the master narrative, and in social media, where one has to compete with a flood of information and large amounts of information noise, elements like surprise, cognitive dissonance, easily recognisable symbols or some eye-catching techniques are used in order to draw the audience into the PSYOPS product.

In PSYOPS the influence over a target group is often achieved by spreading rumours. Those can be:

- Hate rumours: exploit ingrained dislikes and prejudices of a target population.
- Fear rumours: exploit a human tendency to believe the worst.
- Hope rumours: exploit wishes for a favourable turn of events.

Modern technology allows particularly easy exploitation of digital material in order to produce falsified or ambiguous content which can be used for deception and manipulation. Textual messages (posts, status updates, comments) can also be crafted according to the same principles.

Social media provides fruitful soil for PSYOPS as it is largely a trust-based network since it is formed on a networks of friends or like-minded group members. Hence the information coming from an individual or group can be more trusted than that coming from an official mass-media outlet or government communicators. This trust can be manipulated to achieve particular effects. It allows targeting of groups of people connected by certain social ties which increases the chance of the desired effect on perception and behaviour.

It is also very easy to hide the real identity or original source of information on social media as well as manipulate digital data such as imagery. Hence the concept

3 Rebecca Goolsby. *On Cybersecurity, Crowdsourcing and Social Cyber-Attack*. Washington: Wilson Center. U.S. Office of Naval Research, 2013.

of social cyber attack becomes increasingly important as it is based on manipulated information being spread under false identities to networks of users.

4 Understanding Social Cyber Attacks

A social cyber attack, as defined by Dr Rebecca Goolsby, involves acting under false pretences or anonymously, by either releasing a manipulated signal into the social media or by manipulating an existing signal in order to achieve the desired effects: chaos, panic, mass disorders. This type of cyber attack offers a different view to the traditional views on attacks in the cyber environment, as the effects of these attacks are purely psychological.

Spreading rumours is one of the most effective tactics of the social cyber attack, as those can create fear, hate or unfounded hope in the target audience which will most likely result in real-life action: for example, mass protests, withdrawing money from banks, or organised attacks on certain groups or individuals whose image has been portrayed as the enemy.[4]

> *Spreading rumours is one of the most effective tactics of social cyber attack.*

Social cyber attack can also involve traditional hacking if the information to be manipulated and released needs to be obtained or published this way. Since the concept of the social cyber attack is very new, it is often difficult to determine what activity should be classified as one. One might argue that the key component to social cyber attack is the narrative which drives it. The actions by the pro-Russian 'Cyber Berkut' (*КиберБеркут*) and its nemesis, the pro-Ukrainian 'Cyber Hundred' (*Кибersотня*) can serve as examples.

Cyber Berkut is frequently in the news, propagating the Russian political narrative as well as hacking both the Ukrainian Government and other countries. The group successfully attacked and defaced the websites of the North Atlantic Treaty Organisation (NATO) and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), claiming that its activities were in retaliation for NATO support for Ukraine.[5] However, the key to Cyber Berkut's activities is the narrative which it uses to justify and promote its activities. Cyber Berkut claimed credit on its social networking site VKontakte page for hacking electronic advertising billboards in the centre of Kyiv prior to a Ukrainian parliamentary election on 24 October 2014, displaying videos of numerous prominent Ukrainian politicians and labelling them war criminals:[2]

> *[English translation] 'We Cyber Berkut intend to use every opportunity to defend the interests of Ukrainian citizens from the arbitrariness of nationalist*

4 *Ibid.*
5 The post and video can be found here: http://vk.com/wall-67432779_14678

fringe and the oligarchic elite …Today, we have used a few dozen billboards in Kyiv, Ukraine to remind people about the futility of farcical elections …We reiterate once again that no one will change our lives for us. If the people will continue to hope that the authorities in the offices there are people concerned about the problems of ordinary citizens, Ukraine will be more immersed in the chaos of civil war. The United States and the West first brought into the government people who are ready to sell our country to please their owners, and now want to put the same traitors in Parliament. Today, everyone has to realise that his decision depends the future of our country, and the sooner we crack down on neo-Nazi government and deputies, who are just cashing in on this war, the sooner the country's peace and order.'

This narrative was also spread on social media networks. Analysing this statement, one can identify clear attempts to construe enemy images of the Ukrainian Government and induce fear in the population by calling it neo-Nazi and threatening chaos and civil war. The hacking of the billboards had no other meaning than to conduct a social cyber attack by propagating this narrative and spreading rumours through manipulated information.

5 Social Media in the Russian-Ukrainian Conflict

During the war in Ukraine, social media has become home to intense conflict-related information updates, impassioned arguments, and debate.[6] The social media space has been abused, and pro-Russian forces have given the world a masterclass.

At the beginning of the conflict, we saw strategic communications in action. Over Twitter and YouTube, unknown attackers released an intercepted phone conversation between the U.S. Assistant Secretary of State Victoria Nuland and Geoffrey Pyatt, the U.S. Ambassador to Ukraine.[7] In one stroke, the perpetrators sought to discredit Western policy and to announce their access to Western lines of government communication. Thus we saw both a technical exploit on an information system and a psychological attack on the West via social media.

During the course of the conflict, Russia's narrative has been tightly scripted and disseminated, both on traditional media (in 'breaking' and 'eyewitness' accounts on television) and in cyberspace via social media. These venues are mutually reinforcing, encompassing older and younger readers with varying degrees of access to technology. For example, one can no longer watch Ukrainian television in eastern Ukraine; similarly, Russian television channels are no longer available in western Ukraine.

6 See, for example, Irina Anilovskaja. *Война: переписка одноклассников*, Alfra Reklama, 2014.

7 Anne Gearan. 'In recording of U.S. diplomat, blunt talk on Ukraine' *Washington Post*, 6 February 2014, https://www.washingtonpost.com/world/national-security/in-purported-recording-of-us-diplomat-blunt-talk-on-ukraine/2014/02/06/518240a4-8f4b-11e3-84e1-27626c5ef5fb_story.html.

On social media, pro-Russian voices have systemically cultivated fear, anxiety, and hate among the ethnically Russian (and other non-Ukrainian populations) of Ukraine. They have manipulated and distributed images of purported atrocities by the Ukrainian army, including: mass graves of tortured people, civilians used for organ trafficking, burning crops to create a famine, recruiting child soldiers, the use of heavy weapons against civilians, and acts of cannibalism.[8]

Via social media, such information – whether offered with some evidence or merely in the form of rumours – often criss-crosses the globe in minutes, and a well-organised social media campaign can easily influence a target population's perceptions and behaviours.

The Latvian media company LETA conducted an analysis of Twitter posts during the first six months of 2014, and identified an increasing polarisation between pro-Russian and pro-Ukrainian social media users as the conflict escalated, especially following the violence in Odessa.[9] The researchers wrote that 12.2% of all tweets related to the conflict in eastern Ukraine were 'aggressive', dominated by pro-Russian stances, most intense relative to human casualties, and included epithets such as 'fascist' and '*ruscist*'.[10]

Numerous social media postings appear to be disseminated in order to manipulate people in eastern Ukraine.

The conflict in Ukraine has seen numerous social media postings that appear to be deliberately disseminated in order to manipulate people in eastern Ukraine and beyond. During the May 2014 violence in Odessa, someone posted the following to Facebook:

> *[English translation] 'Hello. My name is Igor Rosovskiy. I am 39 years old. I live in the city of Odessa. I have worked as an emergency physician for 15 years. Yesterday, as you know, there was a terrible tragedy in our city, some people killed other people. They killed them in a brutal way by burning them alive, not in a drunken stupor, not to get their grandmother's inheritance, but because they share the political views of nationalists. First they brutally beat their victims, then burned them alive. As a doctor, I rushed to help those whom I could save, but the fighters stopped me. They didn't let me go to the wounded. One rudely pushed me, promising that I and other Jews would suffer a similar fate. I saw a young man I could have saved if I could have taken him to the hospital, but my attempts at persuasion were met with a blow to the face and lost glasses. In fifteen years I have seen much, but yesterday I wanted to cry, not from the blows and humiliation,*

8 More information about the false information related to Russian – Ukrainian can be found at *StopFake.org*, 21 August 2014, http://www.stopfake.org/en/russia-s-top-100-lies-about-ukraine/

9 G.C. 'Ukraine's murky inferno: Odessa's fire examined.' *The Economist Eastern Approaches blog*. 8 May 2014, http://www.economist.com/blogs/easternapproaches/2014/05/odessas-fire-examined.

10 '*Ruscist*' is an invented word with offensive meaning, a combination of the words 'Russian' and 'fascist'.

but from my helplessness in being unable to do anything. In my city, such things did not happen even during the worst times of Nazi occupation. I wonder why the world is silent.'

The Russian-language social networking website *Vkontakte* saw more than 5,000 shares of this post within 24 hours, and it was quickly translated into English, German, and Bulgarian. However, analysts subsequently discovered that Dr. Rozovskiy's profile picture was actually that of a dentist from the North Caucasus, and now believe this social media post to be a hoax.[11]

On 4 June 2014, Pavel Astakhov, the Children's Ombudsman under the President of the Russian Federation, announced on his Instagram account that 'more than 7,000' Ukrainian refugees had fled Ukraine and arrived in the Rostov Oblast in the previous 24 hours. The next day, that number had risen to 8,386. Russian mass media reported these numbers, but Rostov authorities apparently contradicted them, where the Governor's office reported that the number of refugees did not exceed 712.[12]

In July 2014, 3-year-old boy was allegedly tortured and crucified by the Ukrainian military in a public square in Slovyansk, Ukraine. The Russian state-run TV *Channel One* broadcast the 'eyewitness' testimony of Galina Pyshnyak, who stated that she and others were forcibly brought to the central square to witness the public execution. The interview took place at a refugee camp in Russia's Rostov region and was widely disseminated on social media.[13] However, Russian journalist Yevgeny Feldman of *Novaya Gazeta*, as well as journalists from Russia's independent channel *Dozhd*, challenged the report with contradictory testimonies from multiple interviews in Slovyank, in which numerous residents denied any knowledge of the incident.[14]

Throughout 2014, the list of rumours from eastern Ukraine grew to be quite long: the Kyiv government and European Union were building concentration camps; the forest was full of right-wing killers; the May 9 Victory Day holiday had been cancelled;[15] property would be confiscated; and use of the Russian language was prohibited. On one occasion, terrified locals called the Donbas Water Company after social media informed them that the region's water supply had been poisoned.[16]

These stories can be contrasted with the 'Polite People' campaign on *Vkontakte*, which supported the Russian invasion of Crimea with pictures of Russian troops posing alongside girls, mothers with children, the elderly, and pets.[17]

11 'Odesa Doctor Or Random Dentist? Claims Of Atrocities, Anti-Semitism Face Scrutiny,' *Radio Free Europe/Radio Liberty*, 27 June 2015, http://www.rferl.org/content/ukraine-unspun-odesa-doctor-dentist-false-claim/25372684.html.

12 'Rostov officials refuted information about thousands of Ukrainian refugees,' *StopFake.org*, 6 June 2014, http://www.stopfake.org/en/rostov-officials-refuted-information-about-thousands-of-ukrainian-refugees/.

13 'Беженка из Славянска вспоминает, как при ней казнили маленького сына и жену ополченца,' Первый канал, 12 July 2014, http://www.1tv.ru/news/world/262978.

14 Евгений Фельдман, Жители Славянска – о том, был ли распятый мальчик Первого канала на самом деле (w/eng subs), 13 July 2014, https://www.youtube.com/watch?v=UA1LE6iKMfk.

15 Lily Hyde, 'Rumors and disinformation push Donetsk residents into wartime siege mentality,' *Kyiv Post*, 3 May 2014, http://www.kyivpost.com/content/ukraine-abroad/rumors-and-disinformation-push-donetsk-residents-into-wartime-siege-mentality-346131.html.

16 *Ibid.*

17 NATO Strategic Communications Centre of Excellence. *Analysis of Russia's Information Campaign against Ukraine*, 2014.

6 Troll Farming

Who tweets in support of politics? Who posts Facebook updates in support of military operations? Of course, there are millions of true believers in the world, adherents to every cause under the sun. However, it is also possible to fabricate support for anything, especially in cyberspace. The social media offers great opportunities for state and non-state actors to use fake identities or automatically generated accounts to disseminate their narrative to audiences as widely as possible.

On 24 May 2014, hacked and leaked email correspondence (revealed on b0ltai.org) allegedly from a company called the 'Internet Research Agency' in St. Petersburg, Russia, offered evidence of the existence of a professional 'troll farm', including the firm's relationship to the Russian Government. Media reports suggested that recruitment of employees had occurred prior to the onset of military operations, and that workers were tasked with writing 100 internet posts per day.[18]

For strategic communications, these developments are critical to understanding modern information operations including disinformation and PSYOPS, as a well-orchestrated social media campaign could significantly affect the prevailing political narrative.

It is possible to analyse the social media domain in an effort to separate fact from fiction, to investigate when accounts were created, whether they have credible content or a real networks of real friends, but to do this accurately and in a timely manner is an extraordinary challenge for anyone, including law enforcement and counterintelligence organisations.[19]

7 Conclusion

The suspicious and seemingly targeted use of social media in the Russian-Ukrainian conflict offers considerable evidence that social media is being extensively used to support military actions on the ground. To some degree, the information operations have generated fear, uncertainty, and doubt about the economic, cultural, and national security of Ukraine, especially in the eastern provinces where there are strong historical ties to Russia.

> *Social media is extensively used to support military actions on the ground.*

The goal of these social media operations may be to convince Ukrainians that the *Euromaidan* movement has led only to political chaos in the country, and has not been in Ukraine's best long-term interests. This message can be contrasted with

18 Александра Гармажапова, 'Где живут тролли. И кто их кормит', *Novaya Gazeta*, September 9, 2013, http://www.novayagazeta.ru/politics/59889.html.

19 Kenneth Geers and Roelof Temmingh. 'Virtual Plots, Real Revolution,' *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Kenneth Geers and Christian Czosseck, 294-302 (Tallinn: NATO CCD COE, 2009).

some examples of social media commentary from Crimea: that its incorporation into Russia has led to safety and stability on the Crimean peninsula.

The use of cyberspace both to attack the infrastructure and to influence 'people's hearts and minds' is a new phenomenon that has been increasingly used in recent conflicts to support military operations on the ground. This kind of warfare will not disappear; on the contrary the combination of actions which are targeted at infrastructure and human psychology will be used in more sophisticated and unpredictable ways in the future. A three step approach could be recommended for security experts and national decision makers to prepare better to meet these kind of challenges:

Identify. Governments and defence organisations should enhance their capabilities to identify the detrimental use of social media. Information campaigns which entail propaganda and automated or fake accounts to rapidly disseminate information should be closely monitored and analysed. This also includes additional efforts in order to understand how these campaigns are organised and what effects they can have on public perception.

Challenge. Examples by citizen journalists have shown that revealing false facts to the public is an effective approach in mitigating the effects of disinformation. At the same time it is important not to engage in counter-propaganda as this fuels the information war and creates public distrust rather than diminishing the power of misinformation. Humour perhaps could be more helpful in countering aggressive propaganda as it hampers the ability to achieve its aim – subduing the society of the target country. The initiatives in Twitter like @DarthPutinKGB or @Sputnik_Intl are good examples of how to challenge Russia's disinformation campaign with irony and jokes.

Learn and prepare. The development of the unifying strategic narrative – the story which entails the set of the values and beliefs of your country or organisation – is the best defence against propaganda which questions them. A long-term educational effort to enhance critical thinking and media (including social media) literacy would also contribute greatly to society's self-defence against manipulation.