© Gemesi, G. (2020): Hybrid warfare and disinformation in the post-truth era. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): Proceedings of FIKUSZ 2020, Obuda University, Keleti Faculty of Business and Management, pp 208-217 http://kgk.uni-obuda.hu/fikusz

Hybrid Warfare and Disinformation in the Post-truth Era

Géza Gémesi

gemesi.geza@hm.gov.hu; drgemesigeza@gmail.com

Abstract: In this paper I explain hybrid warfare and its methods, focusing on disinformation as one of the most effective and actual way of weakening and destabilising one entity's adversary, mostly other states and belligerents. I give a quick overview of how this mean of warfare has been currently used by states, focusing on Russia, China, and Iran. I come up with the concept that this tool of warfare is significantly effective and its targets are particularly vulnerable these times, often labeled as the post-truh era.

Keywords: hybrid warfare, information warfare, disinformation, Gerasimov-doctrine, post-truth, fake news

1 Hybrid warfare

1.1. How the concept has evolved

Hybrid warfare is an emerging, but ill-defined notion in security studies. It refers to the use of unconventional methods as part of a multi-domain warfighting approach. These methods aim to disrupt and disable an opponent's actions without engaging in open hostilities, and by keeping the level of conflict under the threshold of war.

While the concept is fairly new, its effects and outcomes are often in the headlines today. Russia's approach to Ukraine is an example of this form of warfare. It has involved a combination of activities, including disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure and military actions.

The term hybrid warfare originally referred to irregular non-state actors with advanced military capabilities. (For example, in the 2006 Israel-Lebanon War, Hezbollah employed a host of different tactics against Israel. They included guerilla warfare, innovative use of technology and effective information campaigning.)

© Gemesi, G. (2020): Hybrid warfare and disinformation in the post-truth era. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): Proceedings of FIKUSZ 2020, Obuda University, Keleti Faculty of Business and Management, pp 208-217 http://kgk.uni-obuda.hu/fikusz

First notion of the term was in the early 2000's, when William Nemeth observed the tactics of operations carried out by local warriors in the Chechnyan wars. He recognized that the archaic social order of Chechnya resulted in a way of waging war in which the modern military discipline and tactics (based on the Soviet training and education) assimilated with the forms of armed violence from the era before early statehood. Modern weaponry and technology was used by the Chechnyan rebels, blended with warfare without any legal or moral restrictions. [1]

In 2007, American defence researcher Frank Hoffman [2] expanded on the terms "hybrid threat" and "hybrid warfare" to describe employing multiple, diverse tactics simultaneously against an opponent.

Hybrid warfare carried out by Russia or any other actors are different from that of Chechnyans, however, the use of legal and illegal acts of violence plays a key role in all of them, in terms of both theory and practice. [3]

The meaning of the term was later expanded by John J. McCuen, who observed, based on the experience of the theaters of war in Vietnam, Iraq and Afghanistan, that the USA's strategic aim should be the victory in not only in the physical, but also in the mental dimension. To reach this aim to convince the local population in the war theater and also maintaining the moral support of the homeland's citizens are necessary. [4]

Istvan Resperger noted that hybrid warfare was a flexible use of conventional, linear methods along with unconventional and non-linear ones. The aim of this mixed usage is to destabilize the adversary's state, make its armed forces non-operational, along with keeping the level of violence under the threshold of war.[5]

A. Jacobs and G. Lasconjarias think that there is a wide range of various tools available apart from conventional military power to reach the strategic aim; these are economic pressure, humane and religious means, intelligence services, sabotage and disinformation. Combination of these forms up a highly effective, yet almost invisble ability to destabilize the opponent – and this powerful set of non-conventional weaponry does its damage operating mostly in the non-physical sphere.[6] This paper focuses on the disinformational aspects of hybrid warfare, its methods and effects.

1.2. The Gerasimov doctrine

In February 2013, General Valery Gerasimov—Russia's chief of the General Staff, comparable to the U.S. chairman of the Joint Chiefs of Staff—published a 2,000-word article, "The Value of Science Is in the Foresight," in the weekly Russian trade paper Military-Industrial Kurier. Gerasimov took tactics developed by the Soviets, blended them with strategic military thinking about total war, and laid out a new theory of modern warfare—one that looks more like hacking an enemy's society

than attacking it head-on. He wrote: "The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. … All this is supplemented by military means of a concealed character."

The article is considered by many to be the most useful articulation of Russia's modern strategy, a vision of total warfare that places politics and war within the same spectrum of activities—philosophically, but also logistically. The approach is guerrilla, and waged on all fronts with a range of actors and tools—for example, hackers, media, businessmen, leaks and, yes, fake news, as well as conventional and asymmetric military means. Thanks to the internet and social media, the kinds of operations Soviet psy-ops teams once could only fantasize about—upending the domestic affairs of nations with information alone—are now plausible. The Gerasimov Doctrine builds a framework for these new tools, and declares that non-military tactics are not auxiliary to the use of force but the preferred way to win. That they are, in fact, the actual war. Chaos is the strategy the Kremlin pursues: Gerasimov specifies that the objective is to achieve an environment of permanent unrest and conflict within an enemy state.[7]

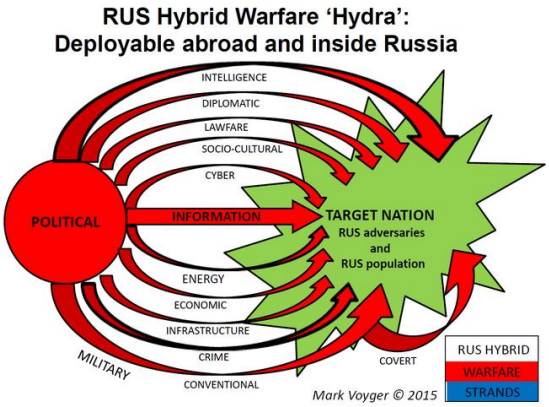

Figure 1
Various tools of hybrid warfare (Russia)

2 Disinformation and propaganda as a tool in interstate conflicts

2.1. Terminology

Much attention has been given recently to the Russian informational warfare activity since the beginning of the Ukranian conflict, and especially since there were allegations that Russia interefered into the 2016 US elections. Since there is an increased media attention regarding the subject matter, I find it useful to give some thought to the terminology itself, and make an attempt to underline the differences between the terms information warfare and disinformation.

Information warfare: information warfare was originally an american military term. It got into wide use in the early 90's at the time of the Gulf war – it meant the struggle for the possesion of information, informational systems and the use of info as a weapon. Now it is used to refer to the activity that includes battleground informational activity, cyber-warfare, propaganda, ideological warfare, also influencing through mass media and "big data" info collecting.

Disinformation: on the contrary, disinformation is a term originating in Soviet military language. Vasilij Mitrohin, a dissident and a former KGB librarian explained that it meant deception through false information, and active intelligence measures too. General Mihail Pacepa, a dissident from Ceausescu's Romania noted that even the name is misleading: Stalin intentionally gave the activity a French-sounding name, thereby suggesting that it was a Western invention. [7]

2.2. Psychological factors

The success of psychological warfare lies in the way the recipient consumes and processes information. Christina Nemr and William Gangware made an excellent study what psychological characteristics, cognitive processes work in the background of disinformations significant effectivity:

- selective exposure leads the individual to prefer information that confirmes their already existing perception;
- confirmation bias makes information consistent with the preexistent beliefs of one individual more credible;
- motivated reasoning works in the inverse way and initiates higher scrutiny to the information that is nonconsistent and with the individuals beliefs;

- naïve realism leads the recipients to believe that that their perception of the reality is the only accurate one, and those who disagree are irrational and disinformed. [8]

2.3. Impact points of disinformation

False information can mostly recognized related those subjects, that are dividing, polarising, contradictory ones within the public opinion of a population. That means that the fake news industry very often disseminates information that flows along the dividing lines of societal cleavages. These typical dividing subjects are the following:

- national identities vs. cosmopolitan identies;
- EU sceptics vs. EU optimists;
- nostalgia towards communism vs. advocates of economic liberalism (especially in former Eastern bloc countries);
- non-educated segments of society vs. well educated elites;
- urban vs. rural population;
- anti-racist vs. strong right wing population;
- anti-migration vs. open society supporters.[9]

What is the exact purpose? As we can see the fake news industry – especially Russian fake news industry – is aimed to reshape social and identitarian groups, to strenghten polarisation and to raise the level of dividedness within a society, by emphasizing the already existing societal cleavages. Also, it can be a powerful tool to plant mistrust between friends and allies, thereby making common efforts and effective cooperation more difficult.

This activity typically leads to a goal: to delegitimize military, political and economical alliances (mostly the EU and NATO and the pro-Western elites), also, to undermine public trust in the institutions of a state: political, judicial system, law enforcement and healthcare.

This goal is even easier to reach in a society, where objective facts are less important and have lesser influnce than emotions and beliefs.

2.4. Post-truth

What exactly is meant by the term post-truth? Paradoxically, post-truth is among the most-talked-about yet least-well-defined meme words of our time. Most observers in the English-speaking world cite the 2016 Word of the Year Oxford

English Dictionaries entry: post-truth is the public burial of "objective facts" by an avalanche of media "appeals to emotion and personal belief".

We can say that "post-truth" is not simply the opposite of truth, however that is defined; it is more complicated. It is better described as an omnibus term, a word for communication comprising a mixture or assemblage of different but interconnected phenomena.[10]

3 Examples of disinformational acts

3.1. Russia

The level of public awareness of informational attacks has been raised when it came to light that there was an intentional and planned influence campaign, ordered by Vladimir Putin to undermine public trust in the US electoral process.

Russian efforts to influence the 2016 US presidential election represented the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.

US Office of the Director of National Intelligence concluded in a report that Putin and the Russian Government developed a clear preference for President-elect Trump, helped the President-elect's election chances by discrediting his opponent Secretary Clinton, and publicly contrasting her unfavorably to him. Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates.

When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency. Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls." Russia has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.

Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties. The Office assessed with high confidence that Russian military

intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com.[10]

One example of earlier of Russian influence campaigns – in accordance with the Office's hint to earlier disinformational acts - can be the late 1980's media campaign related to the AIDS disease. During this campaign the Soviet Union tried to convince the world's public that the AIDS virus was created by the United States as a biological weapon. Aim of this campaign was to strengthen anti-American feelings in the third world countries that were heavily affected by the virus – so it made global cooperation more difficult. Also, it was an effective way to avert attention from the fact that the Soviet Union was itself developing biological weapons. The fake news first appeared in an Indian newspaper that was supported by the Soviets, and later on during the 80's it was published many times by Russian newspapers and by Radio Moscow, broadcasted in African countries.[11]

We can have a perception how nowadays the social media outlets can provide an opportunity to carry out these kind of operations in an increased volume and in a more sophisticated manner.

3.2. China

As we have seen in Russia's interference in the 2016's electoral campaign, its activity is mostly carried out in the cyber domain. China, also uses propaganda in reshaping the US political conversations, but in a slightly different manner.

Example for this is a case that happened in September, 2018 in the state of Iowa. The newspaper China Daily sponsored a four-page advertisement in the Des Moines register, that looked like an actual newspaper spread (two opposite pages facing each other), with journalistic articles. The articles highlighted the advantages of free trade with China, the risks of the increasing tensions of the US-Chinese trade conflict, and also, President Xi's long-time ties to the state of Iowa. That happened in the middle of President Trump's agricultural debate with China, and the midterm campaign. From this it is clear that China makes sophisticated efforts to shape political public opinion in the US. [12]

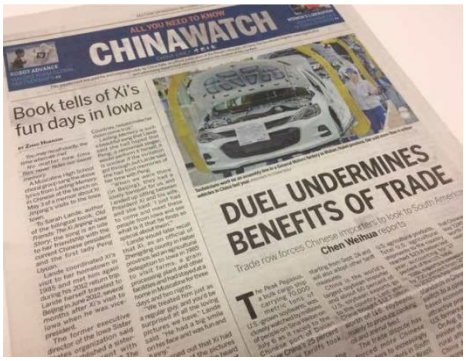

Figure 2
Chinese propaganda advertisement disguised as journalistic article

So slightly differently from Russia's activites, China's international influence campaigns are largely characterized by economic, political and personal relationship-building. Chinese campaigns have been widespread, they range from the global distribution of pro-Chinese media, to attempts to influence educational and policy institutions abroad, to the wielding of financial influence through aggressive loans and infrastructure investment.[13]

3.3. Iran

Iran also prefers using the techniques of hybrid warfare and propaganda in confronting its adversaries. In 2018 two separate Iranian propaganda campaigns were cracked down by Facebook. The propaganda activity was carried out by hundreds of Facebook and Instagram accounts, pages and groups, some of them had been active for than 7 years. The propaganda campaign was similar to Russian and Chinese ones. They used fake accounts to coordinate and disseminate disinformation during the 2018 midterm elections, very similarly to the Kremlins efforts in influencing the 2016 presidential campaign. The Iraninan propaganda largely focused on promoting the interests of the Iranian government – the fake accounts disseminated fake information in a largely anti-Israeli, pro-Palestinian tone, and also included condemnations of Iran's main adversary, Saudi Arabia.

There was an investigation carried out by Reuters whose findings were that Iran maintained more than 70 disinformational websites that reached more than a million followers and etc. 500.000 monthly visits in 15 countries, including the US and the UK.[15]

AWDnews, which was one of these sites, forged a fake piece of information that Israel threatened Pakistan with the use of nuclear weapons once Pakistan sends troops to Syria – to this, the Minister of Defense in Pakistan answered with a real

nuclear threat. Fortunately the hoax was quickly compromised and revealed, but for a period of time it significantly raised the tensions in the region.

As I mentioned before, a typical subject of disinformation can often a topic that is significantly polarises public opinion within a society. A good example of this is an Iranian generated meme, coming from the Iranian site called "No racism no war", picturing the well-known actor Tom Hanks with a photoshopped slogan, that is one of the Black Lives Matter movement.[14]

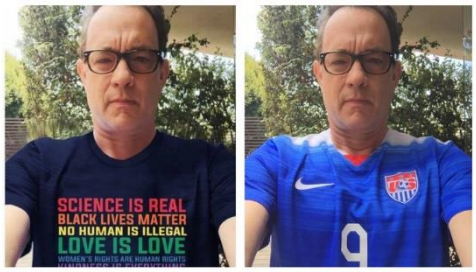

Figure 3
Iranian photoshopped picture for disinformational purposes

The fake photo was later revealed. On the picture the forged and the original is clearly visible.

Iranian disinformational activity is not only political, but also military: Iran's Ministry of Intelligence and National Security systematically releases reports that exaggerates its military strenght and technoligical level. Most possibly, Iran hopes that by boasting with a –fakely - highly effective military power, it can detert any possible enemy actions. Some analysts say however, that Iran's efforts is doing so are of low expertise, and are too suspicious to result in real deterrence. [15]

Conclusions

The concept of hybrid warfare evolved significantly during the last few decades. It was noted by many thinkers, but the concept got the most emphasis from the events of the 2000's. The era in which we are living in is unique from many aspects, but one aspect is more significant than the others, and that is our relationship with information. The methods of hybrid warfare that had been formed by the experiences of the last few decades can and will be more and more effecitve in the future, and this is a challenge that the worlds powers responsible for security will have to face.

References

[1.] Wiliam J. Nemeth: Future war and Chechnya: a case of hybrid warfare. Thesis, Naval Postgraduate School, Monterey, California, 2002

[2.] Frank G. Hoffman: Hybrid warfare and Challenges. Joint Force Quarterly, Issue 52, 1st quarte 2009.

[3.] Jójárt, Krisztián: A hibrid hadviselés és a jövő háborúja, Haderőszervezés, -fejlesztés, Budapest, 2020/1., 5-19. p.

[4.] McCuen, John J.:Hybrid Wars. Military Review, Vol. 88., No. 2., 2008.

[5.] Resperger, Istv:án: A válságkezelés és hibrid hadviselés. Dialóg Campus Kiadó, Budapest, 2018, 21

[6.] Jacobs A., Lasconjarias G. (2015), NATO's Hybrid Flanks Handling Unconventional Warfare in the Sout and East, Research Paper, NDC Rome, No. 112, April https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538

[7.] "Dezinformáció, információs hadviselés, online propaganda: orosz faj?"https://politicalcapital.hu/russian_sharp_power_in_cee/publications.php?article_read=1&article_id=2423

[8.] Christina Nemr and William Gangware: Weapons of Mass Distraction: foreign State – Sponsored Disinformation in the Digital Age, Park Advisors, London, March 2019

[9.] The post-truth age, the fake news industry, the Russian Federation and the Central European area, December 2019Trendy V Podnikání 9(3):46-53, DOI: 10.24132/jtb.2019.9.3.46_53 https://theconversation.com/post-truth-politics-and-why-the-antidote-isnt-simply-fact-checking-and-truth-87364

[10.] US Office of the Director of National Intelligence, „Background to „Assessing Russian Activities and Intentions in Recent USe Elections", The Analytic Process and Cyber Incident Attribution", 06January, 2017,https://www.dni.gov/files/documents/ICA_2017_01.pdf

[11.] US Department of State: "A Report of Active Measures and Propaganda", https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf

[12.] https://eu.desmoinesregister.com/story/money/agricultue/2018/09/24/china-daily-watch-advertisement-tries-sway-iowa-farm-support-trump-trade-war-tariffs/1412954002/

[13.] Samantha Custer et al, „Ties that bind: Quantifying China's public diplomacy and its „good neighbor effect", Willamsburg, William & Mary, 2018

[14.] https://www.politifact.com/factchecks/2020/jan/03/facebook-posts/no-tom-hanks-did-not-wear-t-shirt-progressive-slog/

[15.] https://www.washingtoninstitute.org/fikraforum/view/irans-military-propaganda-failures-and-successes