



SECURITY ACADEMY

EDUCATIONAL PROGRAM ORGANIZED BY
EUROPEAN VALUES CENTER FOR SECURITY POLICY
IN COOPERATION WITH STRATPOL AND SSPI INSTITUTES

The role of intelligence services within the framework of hybrid threats

SAMUEL EDUARD ČERNÍK

Author:

Samuel Eduard Černík

Proofreading:

Matúš Jevčák

Marián Maraffko

Michaela Ružičková

Expert Supervisor

Juraj Kulik



The views and statements expressed in this document do not represent the official opinions of the donors or organizers of the Security Academy. The content of this document is a responsibility of the author.

THE ROLE OF INTELLIGENCE SERVICES WITHIN THE FRAMEWORK OF HYBRID THREATS

Mgr. Samuel Eduard Černík

Abstract

Information operations are very closely linked to intelligence fields and the topic of intelligence. This analytical essay describes the role of intelligence services in (dis)information operations, be it their historical, current and possible future operations. In the body of this essay, author defines the topic of information operations, along with specific historical occasions, in which these were successfully or less successfully used by state and non-state actors. To conclude, author shares opinions about possible improvements in the area of information operations, whether it is on the side of offense or defence.

Keyword

intelligence services; disinformation; operations; hybrid threats

1 INTRODUCTION TO HYBRID THREATS

A hybrid threat is defined as a **set of coercive and subversive activities, conventional and unconventional**, military and non-military, that both **state and non-state actors** can use in a **coordinated manner** to achieve specific objectives **without a formal declaration of war and below the threshold of normal response**.

They are characterized by centrally managed intelligence and information operations, activities of non-state actors, including paramilitary groups, or the deployment of the armed forces of a state actor under a different flag or posing as independent contractors. Such activities may begin **before openly declared military operations**.

Some of them are meant to polarize society, bring uncertainty, and thus undermine the legitimacy, credibility, ability of state institutions and the democratic constitutional order to act, and thus have a negative impact on the realization of the security interests of states exposed to them.¹

Others focus on achieving specific tactical goals, such as reducing the capabilities of the enemy soldiers during skirmishes by disseminating propaganda and using military psychological operations.

Goals of these operations fulfil the standard European definition of war: *“War is simply the continuation of political intercourse with the addition of other means.”* The purpose of hybrid operations is rarely a total victory by annihilating the opposing forces. Usually, the entity implementing these tools has a specific goal in mind, whether it is political, social, or personal. It can also be a short-term tactical goal, or a long-term strategical one.

In principle, we conclude that the basic feature of hybrid operation is its hybrid character. Thus, hybrid action is a combination of several vectors of offensive behaviour of a state or non-state actor below the threshold of normal response.

Vectors of hybrid influence include:

- a) Physical operations against infrastructure (sabotage, alteration)
- b) Industrial espionage
- c) Cyber operations
- d) Paramilitary organizations (proxies)
- e) Military exercises
- f) Promoting social unrest
- g) Promoting and exploiting distrust towards the government and democracy
- h) Influencing local opinion leaders
- i) Disinformation campaigns and propaganda
- j) Influencing academia
- k) Influencing and controlling media²

In this essay, we focus only on the topic of **(dis)information and influence operations, as a critical part of hybrid operations**. It is important to understand that **not all**

¹ KONCEPCIA PRE BOJ SLOVENSKEJ REPUBLIKY PROTI HYBRIDNÝM HROZBÁM

² Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model

information operations (or influence operations) **are based on disinformation** (factual untruths). **Some of the most effective information operations were based on factual data.**

Disinformation, information, and influence operations (for the purposes of this essay will also be collectively referred to as **active measures** or **information operations**) are not a new phenomenon. They have been used for as long as there was a civilized human society by specific people aiming to control the decisions of others in their favor. That is why it is not right to say that this is a modern phenomenon. The goals and core operational ideas of the actors have not changed much, but the specific means and the environment in which they operate have.

In the first place the most common categorization of information operation is the so-called **black, grey, and white operations** (this division is also used by the PSYOPS military apparatus of the United States). **White operations** are submitted directly in an official way with a clear attribution (such as ministry of foreign affairs press release, social media post or state media).

Another group are the so-called **black operations**, the essence of which lies in the hidden character of their origin, and if the actor who allegedly carried out these operations is revealed, this actor will deny and obscure his activity with subterfuge and dismissal.

The third group are the so-called **grey operations**, which lie in the middle of black and white operations. According to the definition of Department of the Army documents, *“products that **conceal and/or do not identify a source are known as grey products. Grey products are best used to support operational plans.**”*³

It is important to note that White, Grey, and Black **don't refer to the product's content** but rather the **methods used to carry out the operation.**

As it was already said, disinformation is not a new phenomenon. Ever since the first human learned that it's possible to lie and gain benefits from it, the history of disinformation began. However, disinformation also proved very useful in the larger political, social, and military struggles. Information operations are widely used by politicians in election struggles, even though the phrase is rarely used in that meaning.

For liberal democracies, disinformation (meaning untrue information operations) represents a **double threat**. Being at the receiving end of **large-scale anti-establishment disinformation campaigns** will undermine democratic institutions and giving in to the temptation to design and deploy **disinformation operations will have the same result for the democratic actor as well.**

It appears to be **impossible to be a democratic country and excel at disinformation at the same time** (unless it is done in a more factual way). One reason for it is, that in **democratic countries possible whistleblowers could damage the credibility of the operations** (telling the untruthfulness of the operations to the press), while in autocratic countries **whistleblowing is a criminal act often punishable by death** (all the while the

³ Headquarters, Department of Army: Psychological operations (<https://irp.fas.org/doddir/army/fm3-05-30.pdf>)

press is fully controlled by the state). That is why **autocratic countries very much enjoy this asymmetry of potential and abuse it to fulfil their own geopolitical and political interests.**

It is important to say that **digital technological advancements fundamentally altered the information operations' game.** With the internet, advanced social media algorithms and people spending more and more time online, (dis)information operations became cheaper, quicker, more reactive, and less risky. However, the disinformation operations became **much harder to control and to assess their results.**⁴ This can lead the actor to **overestimate his success and assume his full control of the situation, which he rarely has.**

In this essay, we would like to show examples of (dis)information operations, which were successfully or less successfully used in the history of politics. In the final remarks, we will provide possible improvements for current information environment, to be used by **democratic actors** in the information space to balance the odds.

2 EXAMPLES OF SUCCESSFUL AND UNSUCCESSFUL OPERATIONS IN THE HISTORY OF ACTIVE MEASURES

2.1 Operation Trust⁵

By 1921, the civil war in Russia triggered a **mass emigration of conservatives and anti-communist Russians.** Many of these groups were trying to reinstate monarchy in Russia and published their own periodicals and press.

All-Russian Extraordinary Commission (also known as “**Cheka**”) was lead by Felix Edmundovich Dzerzhinsky at that time. One of his tasks was to destroy counterrevolutionary activities within Russia and abroad.

Dzerzhinsky suggested setting up a **faux-monarchist organization to engage in operational play** with the émigrés and their goals.

First, Cheka arrested and successfully turned one of the émigrés, Alexander Yakushev, to work on their side.

Yakushev would become the leader of the newly created **faux-monarchist organization in St. Petersburg and Moscow.** He would travel to Europe to meet with “like-minded people” **creating important connections.** The operation got its codename “**Trust**”.

The organization was set up with 400 nonexistent members and was called **Monarchist Organization of Central Russia (MOTsR).**

Yakushev had instructions to gain credibility among the groups and he successfully became **widely respected.**

⁴ Thomas Rid, ACTIVE MEASURES, The secret history of disinformation and political warfare, Profile Books 2020

⁵ Thomas Rid, ACTIVE MEASURES, The secret history of disinformation and political warfare, Profile Books 2020

In 1923, as instructed, Yakushev told the monarchists that they should “*move **slowly and conserve their strength**, because the **Bolsheviks were ready to collapse from within**, and they shouldn’t risk everything with premature attacks or acts of terrorism*”. He repeated the belief that **Russia should be reborn from within**. This was used by Cheka to hinder activities of the émigré groups from abroad, solidifying their power in Russia.

MOTsR had also a different purpose along with the main one. In its name, there were many letters sent, aiming to establish contacts with foreign intelligence services and their operatives. Estonian secret service took the bait and **disinformation operations began**. They created **fake and forged statistics and intelligence about Russian military and defence capabilities**. They exaggerated them heavily, aiming to **deter military intervention from the western powers**.

In the main line, Yakushev kept pushing the **waiting game amongst monarchists**, he said that the **MOTsR would be the agent of change in the collapsing soviet Russia** and aiding Western powers would just create **stronger support with Bolshevik nationalists at home, weakening the monarchists effort**.

The operation went on and achieved great successes (among others, capturing and executing a very powerful British asset – Sidney Reilly), but mainly it achieved its specific goal, to **allow Bolshevik government in Moscow to defend potential threats abroad without using military means**.

2.2 Engineering racial division⁶

In the early 1960s, KGB saw an opportunity to weaken their enemy, the US. They noticed that there were tensions in the black and Jewish communities waiting to be abused by information operations. Oleg Kalugin (coordinator of **race-baiting disinformation operations** in New York City station) wrote: “*I knew our propaganda was exaggerating the extent of racism in America, yet I also saw firsthand the blatant discrimination against blacks.*”⁷

The operations consisted of **sending fake KKK hate letters** to local and foreign associations and countries, **threatening foreign diplomats in New York City, especially Asian and Black delegates**.

KGB, however, realized that they can **effectively play both sides of tensions to increase polarization**. They created a **fake African American organization directly agitating against the KKK**, named **African Friends Association**.

The documents disseminated by this **front organization** (similar to MOTsR) consisted mostly of **true statistics and disturbing images of graphic lynching violence**. The pamphlets contained several falsehoods mixed in with true data. They claimed that **African Americans were forced to “pay for their shanties twice as much as whites do for their apartments”**.

⁶ Thomas Rid, ACTIVE MEASURES, The secret history of disinformation and political warfare, Profile Books 2020

⁷ Oleg Kalugin, Spymaster (2009)

Soviets did not stop at creating their own **fronts**, they also **covertly funded existing groups**. To these groups belonged *The Minority of One (far-left magazine)*, which however had no idea, that they were financially supported by the KGB.

This operation showed that **it is very effective to finance, support, and create your own fronts, on both sides of an ideological conflict** (or a racial, social, religious one) to **increase instability and disrupt social cohesion**, manipulating, and shifting the so-called Overton window to the extremes, creating political stalemates (which can be visible in the current US political struggle).

2.3 Disinformation operations using books

There is a longstanding social belief, that used to always be present since the invention of the printing press, that **books are perceived as more reliable and factual** than just **stories, news, and rumours**. For the **artists of disinformation**, this was a perfect vector of influence.

One example would be the *Penkovsky Papers*, **the CIA active measure against the Soviets**. Penkovsky was a GRU spy, working for the CIA from 12.4.1961 to 4.9.1962. He was captured and executed by Soviets in 1963. The CIA, however, wanted to use the current climate to their advantage. The CIA wanted the world to know that Penkovsky was a military officer, decorated in the World War II and he served in military intelligence. The book contained a short biography, along with **a training manual on handling and supervising American agents by the GRU Anglo-American Affairs Directorate**. Large part of the book was **truthful**, mixed with some **falsehoods to increase its damaging value**.

The book contained a report on a massive **moral decay and abuse of power in Moscow**. Book also contained false stories about many Soviet officials, which fit well with the actual reality of the corruption and power abuse that was present.

The book was then sold from a **front organization, Penkovsky Foundation**, and achieved some success and presence.

The Soviets did their fair share of **book operations**. A good example is a book *Who's who in CIA*. After gaining access to **names of some CIA officers and staff**, the Soviet operatives decided to **publish a book described as a "biographical encyclopaedia of 3.000 members of civilian and military intelligence agencies of the USA in 120 states"**.

The operation used **real names and true information about some staff and officers**, but also added **some false claims about specific people** who didn't have any affiliation to CIA.

By adding up **covertly obtained factual information and forgeries**, they created a credible **book that damaged the reputation of CIA and the US, along with some unsuspecting officials and citizens** who were wrongfully accused.

The technique of **covertly obtaining** (hacking, operative work) **factual information** and **blending** it with plausible seeming, but false information, became **very useful in making the target audience believe, or at least not dismiss the narrative completely**.

It is important to note that modern disinformation operations are much less doable in the Western democratic countries, due to increased press freedom and very large potential to backfire at those disseminating them (the risk of whistleblowers and losing the trust of the large public, along with philosophical problems stemming from liberal democracy). That is why state actors of disinformation operations are mostly autocratic countries, in which trust and obedience of the population are forced (and whistleblowing is punished mercilessly).

2.4 Modern disinformation⁸

Today, Russian Federation is using quite known (and many times already mentioned within the text) tools and methods, including **agents of influence, deception, and use of media** (own and foreign ones), **front organizations** etc. – however, most of these methods under today's conditions are getting new contents and meaning.

The former radio clandestine broadcasting operations were replaced by new methods, more digital in their nature. The activity in Ukraine (2014) started by **taking over TV centres, networks, and TV towers to broadcast information on the occupied territories**. Besides, both territorial groups of insurgents are **active on social networks and also have YouTube channels for news broadcasting**.

The use of **religious organizations and their representatives as agents of influence** also increased its scale. Today, Orthodox churches belonging to the Moscow Patriarchate in various countries of the world are becoming the immediate providers of “active measures”, the open platforms of pro-Russian and anti-Western propaganda, while their clergy is fully supporting all Russian actions, sometimes even directly with military equipment in hands.

Disinformation along with its standard concepts is also used by **fringe or extremist groups** (usually non-state), such as Reconquista Germanica, an extremist far-right and possibly neo-Nazi movement. By the claims mentioned in their own self-report, this group had an “army” of 10.845 trolls.⁹ This group of “trolls” was **manipulating public discourse before German parliamentary election in 2017**. The tactics they used consisted of **anti-Merkel memes, hoaxes, far-right hashtags** (along with “hash-tag” pairing to disseminate their material) and more. They were also attempting to abuse the **trending pages** mechanisms on Facebook and Twitter to increase their **reach to more people**. They were directly focusing on **shifting public opinion towards far-right political party – AfD**. The “troll army” managed to get their hashtags to the top of the popular ladder, namely #TraudichDeutschland, #nichtmeinkanzlerin, #merkelmussweg and #reconquista. Even

⁸ D. Dubov et al.: “ACTIVE MEASURES” OF USSR AGAINST USA: PREFACE TO HYBRID WAR Kyiv 2017 Analytical report; Kyiv 2017

⁹ Julia Ebner, Going Dark: The Secret Social Lives of Extremists, 2020

the official accounts of AfD shared some of these hashtags, **amplifying the troll army success.**

The leader account of the “troll army” based their strategy around **demoralization, division, infiltration, sowing defeatism, and lowering the morale of the “enemy”**. He claimed it is important to convince people that **“there is no purpose”, “it is hopeless” or “you should give it up”**. He also supported **posing as an employee of the “enemy”, claiming the person sees the enemy from within, and it is corrupt and impossible to solve.** He claimed that after this first stage, the main purpose is to divide and polarize, motivate the betrayers, and demotivate the trustworthy in order to **sabotage and destroy any movement.**¹⁰ The leader very much praised and worked with a material published by other German extremist groups, the **“Handbuch für MedienGuerillas”** – *Handbook for media guerillas*, which is a strategic handbook on information operations in digital space (the handbook is unfortunately no longer available on the original link).

The Reconquista Germanica is based around a very strict **recruitment process of new trolls**, which undergo a video call screening in front of more people to judge their credibility and possibly rule out infiltrations by intelligence officers or investigative journalists.¹¹

The group also has a **gamified experience for its members**, which contains rewards and increasing ranking system based on **“trolling” success.**¹² This **gamification element is not to be underestimated within disinformation and propaganda community. It can motivate the members but also the “victims” of disinformation to get more radicalized or even join the ranks of “troll armies” themselves.** Similar to this group, **British Islamist website Salafi Media** uses a **“fundamentalism meter”** to monitor and motivate the **engagement of users.**¹³ **Gamification was also present within groups, such as ISIS or Al-Qaeda.**

In a recent study by ISD, the research has shown that only 5% of all active users account for 50% of all **likes on hateful comments in the German news comment section.**¹⁴ This can create a false illusion that most people on the internet **are angry, radical, extremist**, demoralizing the society even more.

In order to understand disinformation, **extremist groups are also a very good outlet to study deeper.** To recruit, indoctrinate their members, and to disseminate their **ideas successfully**, they have perfected the disinformation mechanics used formerly by **intelligence operatives.**

¹⁰ Ibid.

¹¹ Ibid.

¹² Ibid.

¹³ Ibid.

¹⁴ Institute for Strategic Dialogue: HATE AT THE PUSH OF A BUTTON: Right-wing troll factories and the ecosystem of coordinated hate campaigns online (2018)

2.5 Chinese disinformation

The Chinese government had **established the Confucius Institute program** several years earlier, in 2004, **after publication of the “three warfares” doctrine – public opinion warfare, psychological warfare, and legal warfare**. Over the next several years, Confucius Institutes began to pop up across the United States and Europe. By 2009, there were 90 Confucius Institutes housed at US universities — including prestigious institutions like Columbia, Stanford, and Chicago — and a total of 440 across the globe.¹⁵

The core problem was that the **Confucius Institutes stifled open and free debate. Numerous examples of censorship began to emerge at Confucius Institutes across the globe** — such as in Sweden, Portugal, Australia, and Canada — suffocating discussion in classrooms and at conferences. It instructed teachers in Confucius Institutes to **discourage the discussion of issues that were politically taboo in China, such as the status of Taiwan, the 1989 Tiananmen Square massacre orchestrated by PLA forces, human rights, China’s prodemocracy movement, and the status of China’s beleaguered Uyghur population**.

China has a very specific target for its disinformation operations, **Taiwan**. These disinformation operations are aimed at the political opposition (politicians against one-China policy and against Beijing), and attempt to foment dissatisfaction with these leaders, possibly facilitate a change of governance.

3 CONCLUSIONS

It appears that disinformation is a phenomenon, which is not going to disappear for many years ahead. That is why **liberal democracies** need to focus their resources to counter these threats.

Firstly, it is important to **increase the capacities of intelligence and counterintelligence services**, and also increase their **education on the modern digital disinformation along with the technical aspects**.¹⁶

Also, the **population must be educated on the topic of disinformation and be taught specific tools to evaluate the information they receive**. This is especially important for **younger generations, since school systems are already teaching them important tools for their life, so adding another one would be easier**.

Intelligence services **need to become more public in their appearances**, educating the public on current **threats and disinformation operations**. This needs to be preceded by highly skilled **monitoring of the disinformation sphere**.

An interesting tool would be to **create workshops lead by former or publicly known intelligence officers on topics of information evaluation, OSINT, and fact-checking**.

¹⁵ Seth Jones: Three Dangerous Men (2021)

¹⁶ D. Dubov et al.: “ACTIVE MEASURES” OF USSR AGAINST USA: PREFACE TO HYBRID WAR Kyiv 2017 Analytical report; Kyiv 2017

The presence of intelligence service members can promise an increased turnout, thus amplifying the results.

More activity should be put into **counterintelligence efforts focused on the front organizations**, especially their **funding and ties to foreign intelligence agencies**.

In this sense, specific legal barriers of intelligence work should be put **further, to increase intelligence capabilities**. One example would be to allow the Intelligence service to work with **journalist covers and to recruit journalists as HUMINT sources** (which is forbidden under current legislation in Slovakia). However, increasing the capabilities **must be met with an increase in size and depth of control mechanisms, which need to be kept transparent and high in quality**.

There is also an option of conducting information **counter-strikes against the country's ruling elite**. For example, in the near future, NATO and its allies could possibly respond to disinformation campaigns by revealing some of the **overseas properties owned by senior officials in the hostile country** (especially the autocratic dictators), lessening their support in the domestic and international affairs arena. These operations, however, could amplify the problems with the social dynamic and create a polarized, black-white mentality in the adversarial countries, possibly making the long-term situation even worse.

We must, however, add that **this must not be an endeavour taken up by intelligence services or state actors**. Counter-trolling is only useful if done by **informal groups of people, active on social media**.

And, finally, to specifically **counter Eastern-European anti-NATO and anti-EU narratives, it is critical to make a distinction in strategic communication between the terms anti-Russian and anti-Putin**.

Allowing the “alternative” media scene to claim **that the government has anti-Russian or Russophobic** (against Russian ethnicity) **sentiment creates more space for influence operations by state and non-state actors building on this false narrative**.

It is important to communicate that the West **supports the normal every-day Russian people, who crave democracy and freedom, deserve a non-corrupt government and institutions, but Putin as the autocratic leader is not letting those reforms take place to support his own financial and nepotistic needs**.

So, the strategic communication **can in fact be pro-Russian and anti-Putin at the same time, without creating a false dichotomy fallacy** (abused by the “alternative” media).

This will force the “alternative” media to **switch narrative, to a pro-Putin one** (instead of a pro-Russian one), which is **much less palatable by the Eastern-European public**. The argument will be on **their side, to prove that Putin is beneficial to every-day Russians**, which is a much harder endeavour than to defend Russians based on their **ethnicity and nationality**.

