Active measures as the Russian hybrid aggression
in a retrospect. Chosen aspects

Outline of the subject

Political and military pressure by Russia on its closer or further international neighborhood, and its readiness to escalate tensions have become one of the subjects in security discussions for the last years. High level of Russian hybrid threats\(^1\) has been a subject of numerous analyses and articles. But still the reflection on the subject is fragmentary, because it does not embrace all its aspects and symptoms. Most authors tend to concentrate on disinformation and propaganda, i.e. activities in an informative sphere (media and cyberspace). Meanwhile, information pressure is admittedly a dominant but only one instrument of crisis-prone impact of Russia. Very often deliberately provoked intelligence incidents as well as border incidents, migration, events both abroad and domestically (for example conferences, festivals, peaceful camps), parliamentary and presidential elections interference, financial and political support for radical elements and centrifugal trends within the European Union, decision making interference, discrediting politicians unfriendly to Kremlin are pretexts for overt and covert media operations. Such activities during the Cold War were called active measures.\(^2\) If we put them into a hybrid threats paradigm, it makes it possible to look at them from a broader perspective, to diagnose them and counteract them.

Counteracting hybrid threats makes it a challenge for counterintelligence services. It is determined by the complex of resources used by Russia. The threat is both external and internal, domestic and transnational, military and intelligence, which you cannot respond symmetrically. Hybrid operations are carried out by state and non-state actors secretly and semi-overtly with the use of legal and illegal methods. They are carried out both in physical and information and psychological spheres. Military vocabulary (“information war”, “psychological war”, “propaganda war”, “civilization war”, “political war”) used by Russian experts and journalists makes it difficult to fight with them. It suggests that it is a war between parties using adequate measures. Meanwhile, the situations is asymmetric from nature: hybrid operations on a large scale are used by an aggressor, while the attacked – if only because of respect for basic rights and freedoms and state of law values – have to


find other effective countermeasures and counter methods to contrast the aggressor’s narrative their own positive narrative. In NATO terminology it is called a strategic communication. The term “strategic communication”\(^3\) has apparently widened its former meaning (informative security of the battlefield) and has become sui generis methodological foundation of hybrid threats counteracting treated according to one universal standard. In order to have a consistent approach, the European Union took over the NATO terminology.\(^4\)

A genuine renaissance of the topic of active measures\(^5\) observed in the West is caused by the controversial and imprecise terms containing qualifier “hybrid” and also by the attempts of more complex approach to hybrid forms of aggression. Military origin of the terms, as it seems, overrides sometimes the fact that the army is not the only one (and even not the main) participant of a hybrid war: it is used in a limited scope – as an ultimate argument. In this context, a historical term a c t i v e m e a s u r e s accurately reflects a complex nature of this phenomenon and synthesizes different techniques: political, military, intelligence, economic, diplomatic, financial, media and cyber. It also stresses important (if not crucial) role of intelligence services in preparing and creating executing background for Russian influence operations and close links between these activities and acts of defiance, diversion, terrorism, international organized crime and other symptoms of disruptive activities. Regarded as hybrid threats in retrospect it indicates that they are of intelligence nature. Moreover, the term gives a broader political, social and historical perspective to a picture of threats from Russia.

\(^3\) The cited term of s t r a t e g i c c o m m u n i c a t i o n s as well as the others in the text have been defined in: the National Security Bureau (BBN) mini(dictionary). Proposals of the new terms from security area, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propoz/6035...html [access: 5 I 2018]. More on strategic communication Tomasz Kačała, Komunikacja strategiczna, http://sdis.wp.mil.pl/plik/file/Publikacje/kacala.pdf [access: 5 I 2018].

\(^4\) See for example: Joint Communication to the European Parliament and to the Council of 6 April 2016, Joint framework on countering hybrid threats. The document set out strategic lines of NATO and the EU cooperation: enhancing public awareness by forming special mechanisms of exchanging information between Member States and coordination of the EU activities to gain consistent strategic communication; enhancing resistance of the main strategic sectors, like cyber security, critical infrastructure (transmission of electricity, transportation, cosmic space) as well as enhanced security of financial system, public health protection and support for efforts to counteract any extremism and radicalization; crisis prevention, response and overcoming (definition of efficient procedures, including solidarity clause – Article 222 TFEU and mutual defense clause – Article 42.7 TEU in case of a huge hybrid attack); tightening of cooperation between NATO and the EU, as well as other partner organizations in a common effort to counteract hybrid threats, with respect to openness rule and independence of decision making process of each of those organizations.

Two models of Russian discussions on hybrid strategies

1. Military model. In Russian military thought the terms hybrid strategies, hybrid war, hybrid technologies have appeared relatively not long ago. The start of their implementation has captured Michał Wojnowski⁶ and put it in the context of Russian military thought and strategic culture. He brought forward basic assumptions and terms and put them in a geopolitical paradigm. In general, in Russia they are implemented in the military model of reflection on the nature of present war as development of the so called Gerasimov doctrine, following up amorphous concepts of “small wars”, “rebellious wars” and “asymmetric answers”. The author rightly judged the address of the Chief of the General Staff of the Russian Federation during general assembly of the Academy of Military Sciences⁷ in 2013, disseminated in the Russian and international media as information and psychological operation. As he pointed out:

The general words about alleged changes in the ways the wars were to be waged, what reportedly “colorful revolutions” in North Africa and in the Middle East showed, are treated too literally in the West. It is not about innovative way of revolutions incitements (practiced since centuries) but about modern measures used for that purpose. In case of the so called “Arab spring” it was, for example, the use of media on a broader scale, including social networks (Facebook, Twitter), which is a modern solution. The idea of the artificial revolution initiation is not new as such but the tools used for this purpose are indeed.⁸

---

⁷ Contrary to the name Academy of Military Sciences (AMS) is not a scientific institution, although it claims so. It is financed by private sponsors, who get titles of the honored members of AMS. It focuses ca. 15000 experts in the field of security and defense, who – in public – presents themselves as “the real members” and “the members correspondents” of AMS. It was founded by the president Yeltsin’s decree of 1995 as a centre for independent defense studies. Its constant president is army general Mahmut Gareev. Among founder members were Russian Institute of Strategic Studies (being back then within the Foreign Intelligence Service structures), Scientists Committee “For a global security”, Defense Businesses Supporting League, Russian and American University, Russian Association of Industry and Businessmen, International Studies Centre and others. The Academy employed personnel of liquidated science institutions and political and military personnel assigned to the army reserve. Officially under this prestigious name there is an association of analytical and research centers of the military forces, Ministry of Internal Affairs, Border Guards of FSB, Ministry of Emergency Situations and independent experts and journalists specialized in security and defense area. The Academy combines research and study with social and educational activity: since 2008 it has been publishing a quarterly “Information wars”; its members supply media with information and take part in different system projects by law enforcement institutions, the National Council, the State Duma and the Federation Council. Annual conferences are an important platform of vocabulary and narration standardization used next in media campaigns and of contacts between retired officers of the army and active personnel of military information system.
⁸ M. Wojnowski, Mit wojny hybrydowej..., p. 30.
By the way, back then, Valeriy Gerasimov did not speak about hybrid war but about new generation wars, which he described using Western terms like non-military measures and indirect activities with the use of potential of protest from among the local people. Asymmetric indirect activities are due to rely on the country political isolation, economic sanctions, communication routes blockade, intimidating by the use of force and bringing in international troops on the pretext of human rights protection and humanitarian operations. General stressed foremost a particular meaning of information actions and special operations which were a core feature of the colorful revolutions inspired from outside. By the way, the concept of colorful revolutions, leaded reportedly according to the principles of the warfare, appeared also in Gerasimov’s speeches in the Academy of Military Sciences in 2014 and 2015. In 2016 the General used “soft power” to describe Russian hybrid activities and in 2017 he spoke about the so called hybrid method of waging a war as one should regard as equivalent of a non-contact war, which was confirmed in remarks of the authors of Internal Security Review special edition 2015.

Military researchers of a hybrid war notion stress its small usefulness for Russian wars theory on the one hand, and Western geology of hybrid war on the second, which combines elements of conventional war with guerilla war, terrorism and diversion, propaganda and information war. Their analyses on NATO and USA hybrid operations have socio-technical potential: giving a picture of “the gravity of situation” they justify a mobilization model of a country (embracing not only a military and information sphere but also an extensive state management sphere together with legal, cultural, education spheres, in which there is a clear image of an enemy). It was confirmed by the Academy of Military Sciences conference of March 2017. The panelists agreed that the hybrid specific nature of current conflicts is determined by the superiority of non-military measures over armed struggle. They refer to the General Staff of the Russian Federation assessments of its proportion as 1:4 in favor of non-military factors. And it was concluded that (…) conventional wars are waged by losers nowadays.

2. Civilian model. Civilian analysts linked to Russian special services have attempted more dynamically to adapt NATO concepts of a hybrid war. (At this point it should be reserved though, that the proposed division is simplified. In Russia as

---


“military” all possible kinds of military services are described: army, border guards, National Guards, special services and so on. In political language to distinguish them it is used a term from the 1990s: siloviks. Analysts linked to special services noticed an important practical value of this concept. Transforming it into their own narrative and strategic culture they acknowledged information war as the essence of hybrid war and its core. Most theorists of this consideration movement tend to limit a definition scope of the notion taking out elements of armed struggle, i.e. limiting to actions in NATO terminology described as non-military (or non-kinetic). Generally, in this „non-military“ model the three approaches are possible (although they cross with each other mostly, they are complementary):

1) phenomenological,
2) technological,
3) functional.

The most important indicators of the first approach are attempts to define hybrid war, its origin and symptoms on multidisciplinary ground (sociology, political sciences, military sciences, security science, psychology, ethnology and others). As a sociologist, Farhad Iliasov\textsuperscript{11} put among its referents the following:

- propaganda influence on different suitable audiences in the aggressor’s country and in the attacked countries;
- creating and inspiring of separatists and collaborationists groups in attacked countries;
- initiation of unrests and mass protests;
- diversion and terrorist actions carried out by an aggressor together with insurgents;
- secret support for separatists with arms, intelligence, finance and irregular formations activities;
- activities to destabilize and weaken the economy of the attacked country;
- diplomatic support and information backup for special projects.

According to the author the goals of such actions would be occupation, annexation of the territory, change of political regime or the present government. Alexander Bartosz\textsuperscript{12}, while concentrating on the reasons of the current hybrid conflicts, presents a concept of instability catalysts worlwide. They are:

- USA and NATO activities (presence on Russia’s doorstep)
- unilateral use of force in international relations
- unlawful usage of economic sanctions against Russia
- provoking financial and economic crises
- lack of consensus as far as fight with international terrorism is concerned
- global information confrontation and constant improvements of fighting methods in cyberspace
- tensions and chaos in international relations by support for nationalists sentiments, xenophobia, separatism, extremism, religious fundamentalism

\textsuperscript{12} А. Бартош, Разведка России…, ibidem.
• migration crises, problems with drugs and human trafficking
• reinforcement of fight for raw materials and mineral resources (Middle East, Arctic, Central Asia and the Caspian Sea).

In this context Bartosz puts the notion catalysts of decomposition/disintegration processes (diplomatic notes, paramilitary organizations activity). Also, according to him the most powerful catalyst are the so called colorful revolutions, organized in the watershed stage of hybrid war to get a rapid effect of destabilization in the attacked country.

Technological approach is based on the isolation of hybrid war basic dimensions and its mechanisms. Cited above Bartosz features political, diplomatic, information, paramilitary and historical fronts. Igor Panarin adds ethnic front and develops historical front which, in this case, is grotesque. The origins of hybrid operations against Russia, according to Panarin, are in a secret alliance between France, Austria and the United Kingdom (1815) and in founding Russian Masonic lodge in order to carry out a coup d’etat in Russia. Its indication was the Decembrists revolt in 1825 against Nicholas I. Intensified hybrid operation of the Masonic lodge and the British MI6 in the beginning of 1900s resulted in the February Revolution of 1917 and the biggest geopolitical catastrophe in the world, the collapse of the Imperial Russia (second such catastrophe was the USSR collapse). According to Bartosz such beginning dates back to the Times of Troubles (Great Smuta 1598–1613) resulting in (...) hybrid aggression of Poland and Sweden, supported by the Vatican which had realized a plan of creation Polish-Lithuanian-Swedish superpower, partition of Russia and its subordination to the capital of papacy.13

Former GRU analyst, Sergey Devatov14 perceives hybrid war foremost as a war between civilizations of the East and the West. Apart from the warfare he adds finance front (according to Devatov the worldwide finances are a main front of a hybrid war), semantic (war of narration), economic (fight for resources and technologies) and social front (education, culture and sports).

Finance, economic and trade wars were also of interest of Yuriy Bobylov15 what is reflected in his numerous blog posts and in traditional media. Intellectual efforts of this longtime employee of the Soviet secret Military and Industry Commission and, at present, a deputy rector of the Russian State Geological University and a member of the Russian International Relationships Council, is focused on bringing the hybrid information war experiences to other spheres of life (financial, economic, trade, innovations and technologies). According to him, it is the organizational capabilities

of Russian intelligence services, i.e. executive potential working on the basis of the state
and private partnership that have contributed to the effectiveness of information war.

Functional approach linking all the above ideas, is characterized by the form not
the merit. It is characterized by the propaganda language, constant using key words
like influence agent, the fifth column, colorful revolution. One can
come across such approach in official statements of the Russian Federation officials
which give the theory its practical sense. During the session of the Council of the
Heads of Security Organizations of the Commonwealth of Independent States, CIS,
of 19 December 2017 director of the Foreign Intelligence Service, Sergey Naryshkin,
accusing the West of (...) undeclared hybrid war against the CIS countries, stated that
(...) the UK, Poland, Sweden and Baltic countries are in the vanguard of efforts to
transform Russian emigration communities in the so called revolutionary ячейка.16

This is also a current Kremlin political technologists and the so called opinion leaders
approach to interpret the events according to a “Kremlin line”. Aleksei Pushkov, Head
of the Federation Council committee on information policy and cooperation with
the media, commenting in the pro government newspaper amendments to a bill on
Information, information technologies and security of information, meaning that
foreign media can be regarded as foreign agents (a symmetric Russian answer for
making Russian media Russia Today and Sputnik to register in USA as foreign agents)
had commented American move as (...) information component of American hybrid
war against Russia to restrict Russian influence on the course of events worldwide,
undermining status and image of the Russian Federation.17

Functional dimension of Russian considerations are shown in the last release
of mentioned Igor Panarin18, professor of Diplomatic Academy by the Ministry of
Foreign Affairs of the Russian Federation, a former KGB and Federal Agency of
Government Communication and Information (FAPSI) analyst. This well known
theorist of information wars (proponent and the main representative of information
geopolitics) transformed terms and research assumptions used in the past in scope
of the information war into a language of theory of hybrid war waged by the
West against Russia. In fact, they have the same wide range of referents. A model

2017/12/19/naryshkin-na-zapade-iz-rossiyskikh-emigrantov-gotovyat-revolyucionerov.html
[access: 20 XII 2017].
17 https://rg.ru/interviews/3070.html [access: 5 I 2018].
18 И. Панарин, Гибридная война против России...; the same author, Гибридная война.
Теория и практика, Москва 2017. See also the same author: Гладиаторы гибридной войн,
http://ruspravda.info/Gladiatori-gibridnoy-voiny-23791.html [access: 5 I 2018]; Гибридная война:
прошлое, настоящее и будущее, http://novosti.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8%D0%B3%D0%BB%D0%BD%D0%B5%D0%B5-%D0%BD%D0%B0-%D0%B4%D0%BD%01%8F-%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0-%D0%BE%F%1%80%D0%BE%D1%88%D0%BB%D0%BE%D0%B5-%D0%BD%D0%B0%D1%81%D1%82%D0%BE%D1%88%D0%B5%D0%B5-%D0%B8-%D0%B1%83%D0%B4%1%83%D1%89%D0%B5%D0%B5-%D0%BD%D0%B3%D0%BE%1%80%D1%8C-%D0%BF%D0%B0%D0%BD%D0%B0%D1%80%D0%B8%D0%BD/ [access: 5 I 2018].
of a country sovereignty defense by him (requiring enhancement of Russian information presence in all strategically important regions in the world) appeared useful in his considerations on countering Western technologies of hybrid war. In his own hybrid war definition, Panarin took under consideration current trends in discussions on the subject:

Hybrid war – is a set of military and force pressure, as well as political, diplomatic, information, psychological, and technical pressure together with technologies of colorful revolutions, terrorism, extremisms, special services activities and public diplomacy structures realized according to a plan by the state organs, military and political block or transnational corporations.19

According to the author the instruments of hybrid war are as follow: information operations, psychological operations, cyber attacks, economic sanctions, ethnic weapons, organization weapons, financial and information support of opposition and destructive activities of agents of influence located within public authorities. Panarin stresses also that the most important soldiers (gladiators) of this war are special services thanks to the tools they have.

Scientific and publishing activities of authors close to intelligence services confirm they active participation in a political war of Russia with the West.20 It is a constant war. Hybrid non-military tools are the same that the one used in the Cold War and being described as active measures. The same tools are recalled in the context of information, psychological and economic wars. At present, as shows the above discussion, to describe them Russian theoreticians publicize the term hybrid technologies instead of the former information and psychological technologies or non-violent conflict solving technologies.21 Such change of terms does not change their substance: like former ones they give Russians the possibility of double use: as a constructive mobilization and optimization tool, and as a destructive “weapon” (conceptual, information). These, the so-called wars, planned for a long time, require constant renewing of concepts and adjusting to up-to-date reality, mobilization of “soldiers” and training new generations of them. “Hybrid” approach has aroused

19 И. Панарин, Гладиаторы гибридной войны... [acces: 5 I 2018].
21 See for example: А.В., Манойло, Технологии несилового разрешения конфликтов, Москва 2014. Currently there are many synonym words are used like support measures or special influence measures. They have appeared already in the War Doctrine and in the Doctrine of Information Security of 2000; in further texts they have been replaced with the following terms: non-military measures, indirect activities, i.e. subversion, sabotage, organization of irregular military formations, information influence, information and psychological impact, information and technical impact. In the last version of the War Doctrine of December 2014 there was additional term introduced information technologies. It was introduced also into a new edition of the Doctrine of Information Security of December 2016.
a new wave of interest in cold war, there are more and more voices that it had never stopped. It leads to a new ideologization of Russian aggression against Ukraine or in Syria – as a Russian “just” war against the US and NATO. Because of that, stressing the role of law enforcement and intelligence as having mandate and means to fight colorful revolutions – the most important technology of confrontation between the West and Russia, is an important element of current Russian narrative. Such “hybrid” narrative has not become a symbol of a contemporary thinking and acting, on the contrary, it leads to tested methods from the past.

History: active measures as a hybrid strategy

Active measures is a term as much multidimensional as hybrid technologies. This historical term is a kind of facade that covers different forms of influence always dominated by disinformation and special propaganda. They were carried out by different actors, mostly under the supervision of special services. The term appeared in 1960s when ideological struggle of the Soviet Union against the West was high as a complex term embracing such terms as disinformation, subversion, diversion, etc. to hide offensive activities presented as defensive. Active measures belonged both to intelligence and counterintelligence services. Their most comprehensive definition comes from The counterintelligence vocabulary (Moscow 1972)\textsuperscript{22}, issued by the KGB Felix Dherzhinsky High School (Edited by W.F. Nikitchenko). Active measures term (активные средства) has been defined as:

(...) counterintelligence activities to realize what the opponent is up to, in order to be ahead of his unwelcome steps, to mislead them, to take the initiative, to foil their subversive actions. Active measures, unlike security measures regarding for example protecting confidentiality and state or military secrets, are of an offensive nature, allow for detection and breaking insurgent activities at an early stage, push the enemy to expose, allow to impose ones’ will on them, push to act in a hostile environment and in directions desired for counterintelligence. In practice of counterintelligence activities active measures are those activities which lead to creation of agent situations/positions within the opponent’s place or their close circle, operational games with the opponent, disinformation, disgrace and depravation, transfer to the USSR of people of particular operational value, gaining intelligence and so on.

Intelligence definition of active measures gave a former senior archivist for the Soviet Union’s Foreign Intelligence Service, the First Chief Directorate of the KGB, Vasili Mitrokhin, paying attention to their political, economic, military and ideological dimension. He claimed that in the foreign intelligence of the KGB they were defined as:

(…) operational activities with the use of agents to influence internal and external policy of third countries in the interest of the Soviet Union, other socialist countries, worldwide communism and national and liberation movements; to weaken political, military, economic and ideological position of capitalism; to sabotage its aggressive plans in order to create favorable conditions for a successful Soviet Union’s foreign policy and to secure peace and social development.23

Both definitions have the same perception of active measures aims, i.e. influencing the opponent, disinformation, compromising and corrupting with intent to create favorable conditions for a successful Soviet Union’s foreign policy. Disinformation is meant, in a very extensive way, as an influence with words but also as actions.

Special services played the most important role in performing these techniques, mainly because they had tools to formulate strategic goals and tasks of Kremlin, to indicate their outer operators and to finance them secretly. First Soviet disinformation office was created in 1923 within OGPU/NKVD (Joint State Political Directorate/The People’s Commissariat for Internal Affairs). A separate cell for such activities was the “D” Unit (‘disinformation’) established in 1959 within the First Chief Directorate (Foreign Operations), transformed in time into the “A” Service (‘active operations’). Similar structures were organized by the Main Intelligence Directorate (GRU), in which up to 1991 there had been operated the Seventh Directorate (special propaganda); the Chief Political Directorate of Army and Navy, as Oleg Demidov24 writes, had also other branched structures for information war. This presented institutionalization of active measures indicated that different forms of influence were to be linked into a coordinated and planned process. Practice shows significant evolution of Kremlin’s attitude to disinformation strategy as well: from words to actions and from soft methods to hard ones (from information and ideological subversion to hard subversion).

Active measures were a subject of detailed studies by western analysts, experts on psychological war performed by the USSR during the Cold War.25 Limiting the subject, it was described at times as disinformation.26 It was Vladimir Volkoff himself, a French writer, who elaborated an anthology of such kind of texts. In the introduction of the anthology he described disinformation as a “doctrine” (a system of thinking and acting), regarding deceiving as one of the techniques.27 His comments to the texts show precisely goals, methods and measures used in Soviet operations of influence both the public as well as other countries politics. A source of knowledge on the topic is a rich literature translated into Polish by known KGB

27 Ibidem, p. 11.
defectors (Yuri Bezmenov, Oleg Kalugin, Oleg Gordevsky, Anatoliy Golitsyn and others). Rare Russian works are, by its very nature, in more or less disguised way a mythopoeia. They serve as motivation for Russian services as the topic of Soviet active measures is secret in Russia nowadays.


While analyzing activities of contemporary Russian special services one should be aware of the fact that their \emph{modus operandi} has been developed in the beginning of 1920s. It is back then revolutionary ideas and disinformation operations of offensive counterintelligence creators encountered the Okhrana achievements, which officers joined not only emerging intelligence within the Red Army, but also VChKa and later GPU and OGPU. This is the reason why trying to understand contemporary Russian intelligence both on operational arena and as a foreign policy element requires a historical perspective. Only such perspective allows to understand operational instruments used in the past and to draw conclusions from the goals achieved by them.

The above cited text is an example of an excellent historical analysis of diversified tools used by Soviet services against the Second Polish Republic. To destabilize Polish country Soviet services used all accessible tools: from subversive, terrorist and quasi-military measures, a mass anti-Polish propaganda, both in Poland and in the western Europe, to backstage political actions. Destabilization techniques described by M. Świerczek lead to a conclusion that Russians do not use only one modus operandi but they adjust methods to goals. In view of this it is possible to identify some universal rules for Russian intelligence services. Such unchanging rule is for example looking for the adversary’s weak points or sensitive subjects and using them afterwards to deepen divisions in society and to escalate the situation. Long-term influence is a universal rule (process of the Second Polish Republic decomposition had been going on for the whole period if its existence). Changing vectors in propaganda actions accompanying active activities stays unchangeable, although it was Russia that was an aggressor but Poland, according to the then propaganda and agitation, was presented as (...) \emph{predator, grotesque bastard with an imperial syndrome, watchdog, Trojan horse of the West} and so on. The above analysis, apart from already mentioned, allows to distinguish other organizational principles presented as follow.
Tab. 1. Rules used during covert operations (intelligence and organizational).

<table>
<thead>
<tr>
<th>Operational undertakings</th>
<th>Organizational principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass propaganda action to Poles and minorities living in the then Kresy Wschodnie or Kresy (Polish Eastern Borderlands or Borderlands) and territories to the west</td>
<td>Transborder nature (exterritoriality) of information and propaganda activities</td>
</tr>
<tr>
<td>Transfer of provocateurs, saboteurs, agitators, spies</td>
<td>Secrecy and inspiration of an opponent</td>
</tr>
<tr>
<td>Inspiration to riots in the Polish Borderlands</td>
<td>Taking an opponent by surprise and their confusion</td>
</tr>
<tr>
<td>A series of bomb attacks in central Poland, for example on powder magazine in Warsaw Citadel</td>
<td>Emotional influence on an opponent’s society</td>
</tr>
<tr>
<td>Influence on Polish political scene by the Communist party of Poland (KPRP), Belarusian Hramada, parties and parliamentary fractions in the Second Polish Republic</td>
<td>Using one’s own resources as well as opponent’s</td>
</tr>
<tr>
<td>Incitement of turmoil because of economic reasons</td>
<td>Complexity of methods of influence (political, economic, social, etc.)</td>
</tr>
<tr>
<td>Campaign of intimidation of Polish law enforcement (attempts on Police provocateurs)</td>
<td>Weakening of an opponent’s morale</td>
</tr>
<tr>
<td>Treacherous assassinations, plan to murder Marshall Józef Piłsudski</td>
<td>The end justifies the means, rule</td>
</tr>
</tbody>
</table>


From the perspective of history, it may appear that Russian services have not abandoned methods used in the past. First task of the mentioned KGB Unit “D” was to compromise the Federal Republic of Germany as the land of neo-Nazism. There were agents from the East Germany transferred to the West Germany to profane Jewish tombs, paint anti-Semitic slogans on the walls of synagogues, shops and Jewish organizations head offices and to provoke indigenous people to similar acts. In 1959, as John Barron wrote\(^29\), the authorities of the Federal Republic of Germany noted 833 anti-Semitic acts, which was condemned worldwide and undermined the image of the country. It is hard not to see similar situation as far as “monuments wars” are concerned. They turn instantly in anti-Polish, anti-Ukrainian, anti-Lithuanian, anti-Latvian, anti-Estonian demonstrations.

There are many more examples. Nevertheless, it is worth noting that tested mechanisms from the past are bested, diversified, adjusted to current realities and needs. An example of this is the evolution of simulated groups (groups of undercover agents and officers). The first time when such a group was used, as professor Igor Hałagid\textsuperscript{30} writes, in 1918 in an operation known as the so-called Lockhart plot (alleged conspirators were CheKa agents who came forward to a British diplomat). That provocation was used by Felix Dzerzhinsky as an argument against western diplomacy which tried to carry out a coup d’êtat in the USSR. The attempts were widely publicized domestically and abroad. Simulated groups organization (as fabricated independence movement structures and anti-regime) were brought to perfect during the World War II, using them for liquidation anti-Communist communities on the occupied territories (Ukraine, Belarus, Lithuania, Latvia, Estonia and others) and just after the end of WWII – for liquidation anti-Communist underground in countries of the Eastern Block. At present simulated groups appear in places of conflicts (for example in eastern Ukraine or during unsuccessful coup in Montenegro in 2016) in various forms: private military companies, Cossacks organizations, self-defense troops, youth combats or extremist groups, volunteers, special forces without any ranks, etc.

Secret hybrid technologies as intelligence threat

Intelligence operations called hybrid technologies or active measures are not typical intelligence activities because they have nothing to do with information gathering and analysis – they serve Russian foreign, economic and defense policy. Generally, they stand out from the "classic" intelligence activities by their creative nature.\textsuperscript{31} While the first ones apply to decision making after something happens, the second are something is to happen. It is – as A. Bartosz\textsuperscript{32} explains – to project and create the enemy’s future.

New reality and, first of all, abandoning rigid communist ideology after the collapse of the USSR, as well as impetuous social and economic changes widened possibilities of Russian services domestically and abroad. Intelligence service, subordinated directly to the president, performed from the very beginning in the sense of purposefulness. It was guaranteed by the \textit{Law on Foreign Intelligence Organs} adopted in August 1992 and written by the Foreign Intelligence Service. It stipulated that "career personnel may occupy positions in ministries, departments, establishments, enterprises and organizations in accordance with the requirements of this law without


\textsuperscript{32} А. Бартос, \textit{Гибридная война…}, ibidem.
compromising their association with foreign intelligence agencies. If, during the KGB times, the intelligence had been based in foreign posts under diplomatic cover and in recognized western posts (representative offices of Aeroflot Airlines, dealingships, foreign correspondents’ offices), from the time of the Act they could act under cover any political, economic or social organization. The possibilities have been widened by the Russian-speaking diaspora scattered in all post-USSR countries.

New technology development, i.e. new information and communication techniques, common use of computers, growing dependence on IT infrastructure also favored Russian services. It makes information gathering easier but also facilitates manipulations.

Traditionally in their struggle for information (knowledge) Russian strategic intelligence shows a tendency to broaden activities in different areas: political, economic, social, science and technology, sociological, cultural and military. This struggle for information in Russian intelligence doctrine and strategic assumptions has been quickly transformed into information struggle (or more precisely – disinformation) in the areas relevant to intelligence activities. It suffices to recall that the term information struggle appeared in the West only in the middle of 1990s and almost immediately it has been implemented in Russian official documents (it already occurred in Security Information Doctrine and Military Doctrine of 2000). Long tradition of information and psychological measures and current experiences of the two Chechen wars as well as NATO and the European Union enlargement being a challenge, have also favored. They were accompanied by very dynamic information campaigns. It does not come as a surprise that most Russian theorists stress this particular role of information tools on all stages of hybrid operations (as a passive measure – from monitoring course of events to look for inconsistencies and splits in the attacked countries, by planning and choosing executors to its accomplishment and the so called media coverage).

In this context, as J. Bobylov states, creation of mobilization nets of information cannot be overstated (and the underlying intelligence mechanism, public – private partnership and competence building like analytical and executive personnel able to act autonomously), which should be a model pattern for “hybrid activities” in other areas: economic, financial, business and industrial innovations. Stressing a particular role

---

of intelligence. Bobylov distinguishes special operations (performed by intelligence services) and special projects (in which intelligence services are involved). Following special operations he gives the following characteristics:

- destructive nature (liquidation or weakening of the opponent is a goal),
- secrecy and inspiration (secret activities can be either lawful or unlawful),
- lack of dimensional restraints/limits,
- using indigenous people and foreign nationals,
- comprehensiveness („the end justifies the means” rule),
- wide range of methods on different levels of problem solution,
- special executive structure (using both permanent resources as well as one-time organizations, created only for a single action),
- special material security (including financial),
- special procedure of operation management: their independence and anonymity require responsibility delegation from the decision – making center to executive structures,
- variety of methods depending on the goal,
- concentrating on the opponent’s weak points (vulnerabilities),
- surprise and confusion of the opponent,
- planning,
- unlimited use of resources by priority tasks solution,
- information and psychological struggle along with special operations.

It is very difficult to find in Russian literature information on executive measures necessary to perform special operations and special projects. Which is not surprising, no intelligence service nor Kremlin disclose their active role in such kind of operations and projects. Historical research into active measures as well as studies of contemporary mechanisms of disinformation spreading show that they are used by many different entities. They can be divided into two categories: state entities and non-state entities – intermediary (at present called “proxy”). They have been shown in tab. 2.

---

### Tab. 2. Subjects to operations and special projects.

<table>
<thead>
<tr>
<th>State entities</th>
<th>Instrumentalized entities (proxy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence services of the Russian Federation</td>
<td>Associations created by former military officers and functionaries</td>
</tr>
<tr>
<td>Functionaries of other law enforcement agencies and Ministry of Foreign Affairs</td>
<td>Quasi-military groups (Cossacks, combat sports clubs, Night Wolves)</td>
</tr>
<tr>
<td>State administration workers of different levels</td>
<td>Orthodox church</td>
</tr>
<tr>
<td>Diplomatic personnel on Russian diplomatic posts</td>
<td>Russian third sector organizations (like CIS EMO – public diplomacy)</td>
</tr>
<tr>
<td>Personnel of the Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Cooperation (Rossotrudnichestvo)</td>
<td>Russian-speaking diaspora</td>
</tr>
<tr>
<td>State foundations like Russkiy Mir Foundation</td>
<td>International foundations (sponsored by oligarchs, for example Vladimir Yakunin, Konstantin Malofeev)</td>
</tr>
<tr>
<td>Security services of state concerns (Gazprom, Rosneft, Rosatom)</td>
<td>Security services of private concerns</td>
</tr>
<tr>
<td>State analytical centres</td>
<td>„Independent” analytical centers gathering theorists and practitioners</td>
</tr>
<tr>
<td>Associations sponsored by the state (Russian Geographical Society, Military Historical Society)</td>
<td>Criminal groups members), corrupt businessmen</td>
</tr>
<tr>
<td>Cultural associations, friendship and cooperation societies</td>
<td>Subversion troops acting commercially (for example Wagner’s private military company or in social networks (trolling and factories of trolls)</td>
</tr>
<tr>
<td>System political parties (for example Liberal Democratic Party of Russia led by Vladimir Zhirinovsky)</td>
<td>Nationalist and extremist organizations as well as youth affiliations to such organizations</td>
</tr>
<tr>
<td>State media (including Rossiya Segodnya)</td>
<td>Oligarchs’ media (for example Katehon by Malofeev or British “The Independent” and “The Evening Standard”, controlled by Alexandr and Yevgeni Lebedev)</td>
</tr>
</tbody>
</table>

Source: private study.

Subjects mentioned in the table are treated by Russian theorists as the so-called “own resources”. Non-state entities are to join organizational “mobilization networks” as their autonomous elements managed in a particular way. Separate group of entities is made up of those which belong to intelligence assets of Russia abroad. These are
illegals, agents in countries of operational interest, unaware agents called also “useful idiots”, the so called friends of Russia in the West (corrupt politicians and businessmen, networks of people understanding Russia (political parties, ecologists, anti-globalists, pacifists) and others requiring more detailed research. Naturally, stressing by Russians themselves operational capabilities and the role of non-state domestic and international actors as “Russian soft power” makes it to raise a question whether it is not a part of any disinformation operations. In this context, more important appears to be precise indication of different influence centers of Russia, which also play a role of recruitment centers\textsuperscript{35}. It makes it also easier to precise goals and to identify more precisely the areas threatened by Russian activities\textsuperscript{36}.

**Current hybrid technologies: conceptual and organizational basis/grounds**

Active measures, which have been changed \textit{hybrid technologies}, were a subject of a thorough research in the West during the Cold War. Much successful in this field was interdepartmental commission for tackling them by the US State Department acting between 1981 and 1992 under the leadership of vice secretary of the state Dennis Kux. Experts of the commission as well as its members were preparing cyclical reports on Soviet activities. It was Kux himself who tried to classify those diverse instruments by dividing them according to intelligence sources typology into white, grey and black. Perpetration and responsibility for activities in a white area (overt activities, lawful) and in a grey area (with the use of semi-lawful methods, under different kinds of cover) he assigned to Kremlin, and activities in a black area with the use of intelligence technical and personal methods were assigned to the KGB.

This division, as one may think, is very up-to-date despite the fact that Russia has abandoned the idea of changing the world according to ideological preferences, which was initial reason for active measures in the Cold War times. The doctrine model, which is to justify present actions, is as much inflexible; it is based on the setting the Russian world against the West because of the civilization disparity of „Russian world” sometimes widened to „Eurasian world”. Narration based on the so called geopolitical scientific outlook is at the same time very simplified which was shown by the pseudo-intellectual base of the projects and hybrid operations at the beginning of this paper. The narration is also free from the system of values which had not been described by Russia until now. The narration comes down therefore to undermine others’ values. The narrative is determined also by geopolitics: USA and NATO have become „absolute enemies” that tend to challenge Russia’s position as significant point of strength in the world, taking advantage of Russia’s trust and constant humiliating

\textsuperscript{35} Such recruitment under foreign flag carry out also citizens of other countries, what was confirmed by the example of a citizen of Belarus, Alexandr Usovsky. See for example: P. Reszka, M. Tomaszkiewicz, \textit{Jak Kreml finansował skrajną prawicę w Polsce?}, http://www.newsweek.pl/polska/polityka/jak-kreml-finansowal-skrajna-prawice-w-polsce-artykuly,408023,1.html [access: 8 1 2018].

\textsuperscript{36} See:. J. Darczewska, P. Żochowski, \textit{Środki aktywne…}, ibidem, pp. 63–68.
the country by shaping the world by colorful revolutions. Competition between Russia and the USA and NATO has become a universal argument for domestic politics (creating the illusion of constant threat and omnipresent anti-Russian hysteria and Russophobia) as well as foreign politics. Undermining others’ values (like for example Georgia and Ukraine sovereign right to determine their own ways of development and establishing alliances) as well as fight for widening their influence zone, Russia presents it as an act of defending its sovereignty and a mirror answer to a cynical game of the West. Such way of thinking has become a basis for thinking and acting of the Russian Federation and its law enforcement institutions. It is treated as an effective „conceptual weapon”.

As far as organizational basis and organizational weapon are concerned, their substance is a social systems management, including mechanisms of their self-organization, and organization of special projects with the use of different entities described above. In theory, it is described as a paradigm of „reflective management”.

It is clear that modelling the adversary’s social behaviors requires a very meticulous research and knowledge provided by intelligence. According to Igor Eydman, sociologist, intelligence services are admittedly the most important but only one of many executive entities and recruitment centers. Highly developed organizational system resembles a pyramid with President Putin on top of it making all strategic decisions. His instructions are realized by the President’s Administration (for example its vice chief Aleksey Gromov supervising media concern, including Russia Today broadcast and Sputnik agency, i.e. all the propaganda issues directed to organizing „Russia’s friends” abroad). Individual advisers to president supervise the Ministry of Foreign Affairs and law enforcement institutions. These sui generis „command posts” within the president’s administration are then active through huge concerns, social associations, international foundations, individual oligarchs, and so on. Thus the conclusion is that, in the end, it is Kremlin that mobilizes and gives the signal to start or end hybrid wars.

What is new about the topic is that new technologies and new channels of communication are used which have significantly widened possibilities of Russia in this respect. Internet lifted former communication barriers, allowed access to information online and thus enabled services to gain information on the subject. Development of the so called new media (traditional media online and social media) has created possibilities of immediate spreading of false information (issuing the information all over the world, replicate them, getting rid of unnecessary information, imposing one’s own interpretations), giving, at the same time, anonymity to senders and access to recipients without intermediaries. It also got the possibilities to „whiten”

---

37 More on the topic see: M. Wojnowski, „Zarządzanie refleksyjne” jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w., „Przegląd Bezpieczeństwa Wewnętrznego” 2015, No 12, pp. 11–36; the same author: Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w., „Przegląd Bezpieczeństwa Wewnętrznego” 2017, No 17, pp. 11–55.

disinformation: while looking for confirmation of a given information recipient gets it from a few others sources being disinformation as well. Nowadays, it is possible do deliver disinformation not only to humans but also to machines, i.e. bad (harmful) bots managing the traffic on the network and direct it to an aggressor’s information website by changing their positions they rank among search engines (so called good bots). In the result, global network has delivered inboxes with new tools what makes current problems with Russia’s aggressive foreign policy only an enhanced version of the old problems.

Looking at studies carried out during the Cold War and bearing in mind new elements, reinvented arsenal of active measures, i.e. hybrid technologies – according to current terminology – can be presented as follow (tab. 3).

<table>
<thead>
<tr>
<th>Type</th>
<th>Organizational undertakings</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLACK (coordinated by special services)</td>
<td>– getting agents of influence and preparing unaware people for gaining aims of Russia</td>
</tr>
<tr>
<td></td>
<td>– assassination and terrorism</td>
</tr>
<tr>
<td></td>
<td>– fabrication of documents (false documents, fakes)</td>
</tr>
<tr>
<td></td>
<td>– diversionary groups to perform acts of provocation (devastating monuments, memorial sites)</td>
</tr>
<tr>
<td></td>
<td>– quasi-military actions: subversion, secret limited violence</td>
</tr>
<tr>
<td></td>
<td>– inspirations for demonstrations and riots</td>
</tr>
<tr>
<td></td>
<td>– bribing, corruption and blackmailing politicians</td>
</tr>
<tr>
<td></td>
<td>– creating false inboxes and botnets to carry out cyber attacks, propaganda 2.0. and cyber propaganda</td>
</tr>
<tr>
<td>GREY (coordinated by Kremlin)</td>
<td>– instrumentalization and inspiring of different social groups, including political parties and extreme organizations</td>
</tr>
<tr>
<td></td>
<td>– activities via Russian non-govermental sector and international organizations under control,</td>
</tr>
<tr>
<td></td>
<td>– instrumentalization of Russian foundations and associations, e.g. Russkiy Mir Foundation, Russian Historic Association</td>
</tr>
<tr>
<td></td>
<td>– opening pro-Russia portals and financing them</td>
</tr>
<tr>
<td></td>
<td>– troll factories and pro-Kremlin networks creation</td>
</tr>
<tr>
<td></td>
<td>– trolling and activities in social networks</td>
</tr>
</tbody>
</table>
Finally, it is worth to stress once again, that hybrid technologies, known previously as active measures, rooted in tradition and in political as well as in strategic culture of Russia, were of different nature: from ordinary propaganda and disinformation based on frauds to political assassinations and political terrorism. Between them there is a wide grey zone. That zone is a major theatre of Russia’s confrontation with the West aimed at destruction of foundations of the attacked country (administrative, political, social, economic, cultural, etc.). The zone itself is a rather poorly studied area going beyond analyses because of secret and semi-lawful nature of activities (therefore lack of hard facts), lack of proper tools to measure their scale and devastation also because of numerous and diverse intermediaries.

**Summary. Complex nature of Russian threat**

Russia’s activities fit into current security situation, which is characterized by growing significance of non-military threats (just under conventional wars threshold), variability and unpredictability. In NATO strategies they are named *hybrid threats* based within defense area, which does not make it easier to understand their complexity and to counteract them. Described above activities by Russian special services and other „civil” entities are very far from straightforward military dimension so counteracting by military methods is not sufficient. Because of their backstage nature they should be treated as intelligence threats from security area.

Historical term *active measures* reflects in a very good manner cross-sectoral nature of Russian threat. Most techniques of Russian confrontation with external environment are of indirect character and as such are very hard to reach. Their goal is to reach strategic interests and to strengthen international position of Russia and „to disarm” opponents, i.e. to create such situation that domestic actors will be capable of realizing aims of Russia foreign policy. Making use of weak
resistance and hurdles in threats identification, Russia tends to destabilize situation in attacked countries, influences in a destructive way their administrative and decision-making structures, undermines their social and economic foundations as well as cultural background (ideology, system of values, political culture, rule of law). The threat is both internal as well as external, domestic and transnational, to which it cannot be responded symmetrically. Disruptive activities are performed by state and non-state entities, both covertly and openly, lawfully and unlawfully. This is a constant process based on integrated state activity on multiple fronts with the use of different channels (diplomatic, political, economic, military, social, media) subordinated to the long-term strategy of support for Kremlin’s politics.

Strategic narration imposed by Russia blurs boundaries between war and peace, between offensive and defensive activities. Its major goal is to shape the picture of Russia as a victim of cynical play by the West and imposing opinions that it is a war between two parties using the same and adequate measures. Meanwhile, the situation is of asymmetrical nature: the attacked party will be able to assess destruction scale until after its effects. Because long-term goals of Russian foreign policy take into account revision of the present international security system, in the mid-term perspective it should be expected that intensity and scope of activities against NATO and EU member countries will not diminish. Systematic widening of conceptual and executive background as well as including forces and military measures in the so called influence arsenal prove it. It means that crisis-building role of Russian threat will be increasing and its effective repulse will require increased attention of security and defense entities involved and more intensive studies concerning Russian organizational projects, their conceptual assumptions, new techniques of influence, corrupt methods of financing and inventing procedures to quickly and effectively neutralize them. It will allow to avoid thinking that aggressor is schematic: it is a must to be prepared for new, yet unknown, methods of political confrontation.

Abstract

The subject of active measures as elements of hybrid activities strategy has been raised in the article. According to the author historical perspective is useful in recognizing and detecting current operations of Russian special services. Such analytical frameworks of terms make it easier to show some generalizations, they also lead to the conclusion that the activities being a clue of described terms are of constant and complex nature.

Active measures and hybrid technology appearing in the title of the article have the same scope of designates and are collective terms embracing different instruments for political, military, intelligence, business, diplomatic, me-
dia, economic, social and cyber influence to realize long-term goals of the Kremlin policy. Naturally, counteracting Russian threats requires just as complex approach.

**Keywords:** active measures, hybrid war, threats, intelligence, disinformation-subversive operations, covert action.