The CRGN Research Notes

French Gendarmerie Research Center

Issue 109 – December 2024

Captain Pascal Martin (PhD)

©Canva

Priorité stratégique de la prospective

L'avenir des territoires numériques

CRGN certifies that this document was written by a human intelligence

THE REVIVAL OF SOVIET "ACTIVE MEASURES" THROUGH DIGITAL TECHNOLOGY AND THE "RUSSIANIZATION" OF INFORMATION MANIPULATION OPERATIONS

Information manipulation operations are particularly known for having been carried out by the KGB[1] during the Cold War. In Soviet doctrine, they were referred to as "*active measures*" (aktivni meroprijatija), which were defined as "*measures taken by agents aimed at exerting influence on the foreign policy and domestic situation of target countries in the interests of the Soviet Union and other countries of the socialist community […], weakening the political, military, economic, and ideological positions of capitalism, undermining its aggressive plans, with the goal of creating favorable conditions for the implementation of the foreign policy of the Soviet Union*"[2].

Active measures included manipulation techniques, disinformation, propaganda, and the creation of forgeries[3]. They stemmed from a decree issued by Yuri Andropov[4] on April 12, 1982, in which he ordered all intelligence officers of the First Chief Directorate of the KGB, regardless of their current assignments, to take active measures to ensure that Ronald Reagan would lose his re-election campaign[5]. These measures were then used abroad and within Soviet territory, particularly to discredit or slander opponents or dissidents. However, their primary purpose was geopolitical, as they included disinformation as an essential mode of operation, which is "*a psychological warfare operation, primarily intended to influence the policies of foreign governments, to provoke tensions between nations, to discredit certain leaders or institutions, or, in the case of friendly countries, certain opponents*"[6].

But were active measures effective? Are we witnessing their revival in the current geopolitical context? Is there evidence of a "*Russianization*" of these operational methods?

I) The KGB's active measures: a tool used during the cold war

Stanford Turner, former director of the Central Intelligence Agency (CIA), believed that "*if the USSR acted in the industrial and agricultural sectors with the same entrepreneurial spirit it showed in the field of disinformation, it would have surpassed the United States a long time ago*!"[7]. Furthermore, Yves Bonnet[8] considers the record of active measures

1 « *Komitet gossoudarstvennoï bezopasnosti »,* in English « Committee for State Security ». The KGB is the USSR's main intelligence service.
2 MITROKIN, Vasily. *KGB Lexion : The Soviet Intelligence Officer's Handbook,* Londres : Franck Class, 2002, p. 13.
3 LIMONIER, Kévin, AUDINET, Maxime. La stratégie d'influence informationnelle et numérique de la Russie en Europe. *Hérodote,* n° 164, 2017, p. 124.
4 Yuri Andropov was head of the KGB from 1967 to 1982, then General Secretary of the Communist Party Central Committee until his death in 1984.
5 M. ANDREW, Christopher. *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB.* New York : Basic Books, 1999, p. 242.
6 BONNET, Yves. *Contre-espionnage. Mémoires d'un patron de la DST.* Paris : Calmann-Lévy, 2000, p. 268.
7 Statement by Stanford Turner, former director of the CIA, from: LECOMTE, Bernard. *KGB. La véritable histoire des services secrets soviétiques.* Paris : Perrin, 2020, p. 259.
8 Yves Bonnet was Director of the *Direction de la Surveillance du Territoire* (DST) from 1982 to 1985.

and disinformation operations carried out by the Soviets in the 1970s and 1980s to be "*eloquent*"[9], since the USSR, "*a totalitarian state par excellence, possessing the most powerful military force in all of history, was able to craft the image of an emancipating country, supporting oppressed peoples, aligned with the aspirations of the Third World, and a champion of pacifism*"[10]. Oleg Kalugin, a KGB defector, states that the goal of active measures was not intelligence gathering, but subversion. Their aim was to weaken Western countries from within and to foment divisions among them —between NATO member states and neutral European states, as well as between developed countries in Europe and America and developing nations in Asia, Africa, and Latin America[11].
Soviet active measures were based on the interweaving of three types of measures[12]:
– "Black" measures: including clandestine operations, the use of agents of influence, and the creation of false information and fabricated evidence;
– "Grey" measures: involving the Communist Party and its foreign branches, NGOs, research institutes affiliated with the USSR, and clandestine radio stations;
– "White" measures: corresponding to influence exerted through diplomatic actions, financial exchanges, and humanitarian aid.

II) Are we witnessing a revival of the KGB's active measures?

Are we currently witnessing a revival of active measures and their adaptation to cyberspace? The current leaders of the Kremlin are the "*heirs*" of Andropov, most having been recruited by the KGB in the 1970s with the aim of bringing new ideas[13]. Does this background condition the operational methods observed in Russia today?

Richard Dearlove, director of MI6[14] from 1999 to 2004, indeed considers that there has been a transposition of former Soviet active measures into the digital realm[15]. The distinction between black, grey, and white measures now appears applicable to current *modus operandi* when taking into account the possibilities offered by digital tools. Thus, black measures correspond to cyber-clandestine operations conducted by Russian intelligence services, their proxies, or hackers connected to the authorities. Grey measures correspond to influence actions carried out in the informational sphere through blogs, the use of bots, trolls, and agents of influence on social media, with the aim of defending Russian interests, "*re-informing*", and damaging the image of their adversaries. White measures are now carried out within the framework of diplomatic actions, supported by media outlets such as *Sputnik* and *Russia Today*.
Some authors thus observe a genuine reappropriation of the active measures model in cyberspace[16]. The Canadian Security Intelligence Service (CSIS) emphasizes that "*even though information technology in general, and the Web in particular, create new opportunities for practicing disinformation, the rules of the game have not changed much. Like jazz standards, which remain recognizable no matter the musicians and arrangements, disinformation campaigns end up resembling one another*"[17]. The central role played by social media in the dissemination of information and the shaping of opinion thus allows this "*nearly fifty-year-old model*"[18] to be rejuvenated by fully exploiting all the possibilities offered by digital tools. For example, in 2016, Russian services used *Pokémon Go*—the augmented reality game in which users go out and use their phones to find *Pokémon* characters—to encourage activists to gather and express their anger[19].
John Sawers, director of MI6 from 2009 to 2014, also emphasizes this digitization of Soviet, then Russian, active measures[20]. Due to the opportunities offered, the digital era opens up a broad range of possibilities, more effective and less risky than the "*classic*" actions carried out under Andropov[21]. Thus, Russia's historical mastery of active measures is

9 BONNET, Yves. *Contre-espionnage. Mémoires d'un..., op. cit.* note 5, p. 269.
10 *Ibidem.*
11 KROSS, Eerik-Niiles. « America, welcome to the war ». *Politico*, 2 août 2016.
12 LIMONIER, Kévin, GÉRARD, Colin. Guerre hybride russe dans le cyberespace. Hérodote, n° 166-167, 2017, p. 157.
13 HILL, Fiona, G. GADDY, Clifford. « How the 1980s Explains Vladimir Putin ». *The Atlantic*, 14 février 2013.
14 The Secret Intelligence Service (SIS), also known as MI6, is the UK's foreign intelligence service.
15 « *Soviet, then Russian, intelligence has always carried out what it called "active measures" [...]. What is new, however, are the sophisticated technologies it has developed to carry out this interference*.". In : GASTINEAU, Pierre, VASSET, Philippe. *Conversations secrètes. Le monde des espions.* Paris : Fayard, 2020, p. 80.
16 LIMONIER, Kévin, GÉRARD, Colin, *op. cit.* note 11, p. 157.
17 CANADIAN SECURITY INTELLIGENCE SERVICE. *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui.* Site du gouvernement canadien, 2018, p. 27.
18 LIMONIER, Kévin, GÉRARD, Colin, *op. cit.* note 12, p. 157.
19 COLON, David. *La guerre de l'information. Les États à la conquête de nos esprits*. Paris : Tallendier, 2023, p. 183.
20 "*The Russians have increased their capacity to intervene in Western political life. Of course, these are not new techniques [...]. What is new is their use of the Internet, of social networks, which are platforms that have been created with criteria of openness, of free access and not of security or reliability."* In : GASTINEAU, Pierre, VASSET, Philippe, *op. cit.* note 14, p. 81.
21 DECLOQUEMENT, Franck. Actions de cyber-propagande russe en contexte pré-électoral français. *Atlantico*, 28 février 2017.

"*magnified by modern technology [and] respects the basic operational principle, which is to slander and amplify*"[22]. There is, therefore, doctrinal continuity: while the means have changed, the doctrine remains the same, with recourse to a wide range of actions[23] (sabotage, diversion, manipulation, propaganda, state terror, exploitation of the protest potential of the local population). It is thus an adaptation of methods that incorporates new digital tools, making today's Russian information operations a "*clever mix of Soviet-style propaganda and American-style entertainment. There is a mimetic aspect in the Russian approach, which draws on the latest Western communication and public relations techniques".*[24] Hence, "*the more things change, the more they stay the same*"[25].

III) A posture of strategic intimidation

The Canadian Security Intelligence Service (CSIS) considers that Russia has explicitly militarized its disinformation apparatus[26], that the Kremlin's disinformation operations are direct descendants of the KGB's "active measures", and that modern technology only increases their scale, speed, and power[27]. However, some observers offer a more measured assessment. Without denying the link to Soviet methods, "*one should avoid reducing informational actions to a mere tactical modernization*"[28]. These operations are distinguished by innovative procedures and tactics that enable adaptation to the technical constraints of digital networks used as channels of dissemination[29]. Moreover, the transposition of active measures and their adaptation to cyberspace facilitate defamation operations and their amplification[30], as well as the creation, use, and spread of compromising material (kompromat[31]).

Beyond technical procedures, the objective has also changed, since the aim is no longer to promote an alternative ideology as during the Cold War: there has been an "*ideological renunciation*"[32] aimed "*less at convincing than at weakening through division. And from this point of view, Soviet techniques remain useful*"[33]. As a result, from a tactical standpoint, the targets of these actions are most often symbolic, with high geopolitical or political value: the goal is not necessarily their destruction, but the exploitation of the act's media potential[34].

This approach allows for significant media impact in order to multiply the destabilizing effect. The entirety of these informational actions enables Russia to occupy an important place in strategic debates at the international level, while also asserting state power internally and within its sphere of influence. These elements are part of the doctrine of the "information space", which does not focus solely on the technical aspects of cyberspace. Russia is thus implementing "*a true digital influence strategy in that it unfolds across the full spectrum of activities involving the exchange, dissemination, and processing of data, by exploiting networks (of which the most important is the Internet)"*[35]. This digital influence therefore includes a "*posture of strategic intimidation*"[36], notably relying on non-military tools such as disinformation and propaganda actions, and clandestine means of operation[37].

IV) The "russianization" of chinese operational methods

The renewal of Russian active measures has also inspired other powers, including China. The Canadian Security Intelligence Service (CSIS) notes that Russia, China, and the Philippines use information manipulation for domestic political purposes, but that Russia stands out through its sophisticated operations and operational ambitions, aimed at influencing foreign political opinions and destabilizing incumbent governments[38]. However, some authors argue that

22 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 17, p. 7.
23 DARCZEWSKA, Jolanta. « The Devil is in the details: Information warfare in the light of Russia's Military Doctrine ». *Point of View*, n° 50, Varsovie, 2015, p. 7.
24 JEANGÈNE VILMER, Jean-Baptiste, ESCORCIA, Alexandre, GUILLAUME, Marine, HERRERA, Janaina. *Les manipulations de l'information. Un défi pour nos démocraties*. Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) et de l'Institut de recherche de l'École militaire (IRSEM), Paris, 2018, p. 53.
25 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 17, p. 28.
26 *Ibid.*, p. 9.
27 *Ibid.*, p. 25.
28 LIMONIER, Kévin, GÉRARD, Colin, *op. cit.* note 12, p. 151.
29 *Ibid.*
30 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 17, p. 44.
31 JOSSE, Pauline. Le « Kompromat », l'art du chantage à la russe [en ligne]. *France Culture*, 19 février 2020. Available at : https://www.franceculture.fr/geopolitique/le-kompromat-lart-du-chantage-a-la-russe
32 JEANGÈNE VILMER, Jean-Baptiste, ESCORCIA, Alexandre, GUILLAUME, Marine, HERRERA, Janaina, *op. cit.* note 24, p. 54.
33 *Ibid.*
34 LIMONIER, Kévin, GÉRARD, Colin, *op. cit.* note 12, p. 158.
35 LIMONIER, Kévin, AUDINET, Maxime, *op. cit.* note 3, p. 124.
36 MINISTÈRE DES ARMÉES, *Actualisation stratégique*, 2021, p. 17.
37 *Ibid.*
38 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 17, p. 8.

even though the term "active measures" is rarely used to describe Chinese operations, these operations nevertheless "*clearly draw from the repertoire of instruments forged by the KGB to conduct influence operations*"[39].
The Chinese authorities, criticized by the international community and their own population in the context of the COVID-19 pandemic, carried out numerous operations of an informational nature. Indeed, in 2020, Beijing "*spread the rumor that the virus originated not in China but in the United States*"[40]. This operation mirrors the characteristics of the KGB's "Infektion" operation from the 1980s and constitutes, according to the authors of the report, "*a kind of replica*", leading them to name the operation "Infektion 2.0". While there is indeed doctrinal and operational mimicry, the main difference between these two operations conducted 40 years apart lies in the medium of dissemination: cyberspace enables a compression of time and geography, as well as the adoption of a defensive posture by the Chinese authorities in response to accusations.
Indeed, the "Infektion" operation began with the publication, on July 17, 1983, of a letter in The Patriot, a newspaper established in India by the KGB in 1962[41], which was then relayed by multiple outlets and supported by the Stasi[42], before being picked up by some Western media in 1987—four years later[43]. While the Russian campaign had a massive impact, it took four years to become fully effective and, most importantly, did not adopt a defensive posture, unlike the Chinese case. This essential difference stems from the exploitation of new communication technologies, particularly social media, which played a central role as vectors for disseminating manipulated information: the Chinese operation unfolded over the course of just one month[44] and allowed for a high degree of responsiveness in execution.
This operational and doctrinal mimicry has led some authors to adopt the term "russianization"[45] of Chinese information manipulation processes. Furthermore, even without using the term "russianization", the CSIS draws a parallel between Russian and Chinese methods in the informational sphere: their doctrines help solidify their grip domestically and achieve their foreign policy objectives, whether through immediate effects or long-term strategic outcomes[46].

These strategies of information manipulation, when carried out within democratic countries, aim to erode citizens' trust in their institutions and to polarize opinions in order to amplify existing tensions in public debate. Democracy relies on peaceful, contradictory, and informed debate of ideas through freedom of expression and freedom of information. Citizens' trust in the objectivity, transparency, and truthfulness of the information they receive is therefore essential. As a result, information, once a source of power, becomes a power in itself: a powerful lever for states in international relations.
In 2014, shortly after Russia's annexation of Crimea, Hillary Clinton reportedly confided to one of her advisers in these terms: "*Russia is winning the information war in Ukraine and elsewhere […]. They repeat lies endlessly, like in the Soviet era. But they do it on 21st-century platforms. […] It's a global information war, and we're losing it*"[47].

***Pascal MARTIN** is at the head of a department at the National Cyber Unit and a researcher with CRGN and IRSEM. He has a PhD in modern and contemporary history.*

Translated by Aude Grégory, Reserve assistant gendarme

39 CHARON, Paul, JEANGÈNE VILMER, Jean-Baptiste. *Les opérations d'influence chinoise. Un moment machiavélien,* Rapport de l'IRSEM, Paris, Ministère des Armées, 2e édition, 2021, p. 34
40 *Ibid.*, p. 583.
41 UNITED STATES DEPARTMENT OF STATE, « Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87 », août 1987.
42 The Stasi is the former secret police of the German Democratic Republic (GDR).
43 BOGHARDT, Thomas. « Operation Infektion. Soviet Bloc Intelligence and Its AIDS Disinformation Campaign ». *Studies in Intelligence*, vol. 53 , n° 4, 2000, 24 p.
44 CHARON, Paul, JEANGÈNE VILMER, Jean-Baptiste, *op. cit.*, note 39, p. 590.
45 *Ibid.*, p. 589.
46 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 17, p. 8.
47 STENGEL, Richard. « Information wars ». *Black Cat,* 2019, p. 111-112.