Sodobni vojaški izzivi, 2024 – 26/št. 2
Contemporary Military Challenges, 2024 – 26/No. 2

Lawrence E. Cline

DOI: 10.2478/cmc-2024-0010

NAČRTOVANJE STRATEŠKEGA INFORMACIJSKEGA DELOVANJA

PLANNING FOR STRATEGIC INFORMATION OPERATIONS

Povzetek Strateško informacijsko delovanje se običajno obravnava kot vprašanje nad vojaško ravnjo. Kljub temu je bistveno za oblikovanje širšega operativnega okolja in zagotavljanje strateške pobude z izjemo vojne in zato ključno za vojaške stratege. V večini zahodnih držav je bil poudarek na obrambnih ukrepih proti nasprotnikovim prizadevanjem na področju informacijskega delovanja. Takšna obrambna miselnost ima malo možnosti za uspeh. Nekateri dolgoročni vzorci in izkušnje na področju informacijskega delovanja so uporabna podlaga za kampanje obrambnega in ofenzivnega informacijskega delovanja.

Ključne besede *Informacijsko delovanje, dezinformacije, informacijska vojna, politična vojna.*

Abstract Strategic information operations (IO) have normally been viewed as an issue above the military level. Nevertheless, they are critical both in shaping the larger operational environment and in providing a strategic initiative short of war. As such, they are crucial for military strategists. Also, in most Western countries, the focus has been on defensive measures against opponents' IO efforts. Such a defensive mindset is unlikely to succeed. Some long-term patterns and lessons learned in IO provide a useful template for both defensive and offensive IO campaigns.

Key words *Information operations, disinformation, information warfare, political warfare.*

Introduction

Both during the Cold War and since, many countries have been subject to various forms of Information Operations (IO) campaigns. Attention among analysts has been mostly focused on how to defend against such attacks, portraying IO efforts as essentially malevolent (Dowse and Bachmann, 2022; Jones, Simon, 2018). A typical approach has been to place these campaigns under the rubric of political warfare by opponents, and to offer ways to fight them using defensive means (Bagge, 2019; Polyakova and Boyer, 2018).

Defense against IO campaigns is certainly critical, and efforts to improve counter-IO must continue. There are two issues associated with a focus on counter-IO, however. The first, to be discussed in more detail below, is that these efforts may in fact prove counterproductive. The second, broader, issue may be even more critical. This is that focusing solely on counter-IO – usually described as fighting disinformation – cedes the initiative to the opposing countries. Trying simply to counteract the efforts of others can prove to be an exercise in futility. Understanding some of the critical processes in developing IO campaigns is crucial, both to disrupt the opponents' efforts and to conduct our own IO efforts.

After briefly discussing current IO processes at the purely military level, this paper focuses on IO at the higher strategic level. Although most of these efforts are not conducted by military elements, they are critical in the broader strategic context. It may also be noted that many of the examples of IO campaigns date back to the Cold War. This is very deliberate, because there has in fact been a continuity of approaches and types of campaigns for many years. In the case of Russia in particular, much of its conceptualization continues to reflect that of the Soviet Union. The tools for dissemination have, of course, both changed and improved, making IO campaigns easier, but the tools should not be confused with the underlying thinking. The focus in this paper is on Soviet-bloc and, subsequently, Russian IO operations, both because these are viewed as the more significant threats and because there is considerable open-source information available on these efforts. Most of the threats and responses can certainly be applied more broadly, but the primary emphasis in this study is on Russia. The methodology employed is the use of available open-source historical information and current reporting and analysis.

1 INFORMATION OPERATIONS AT THE MILITARY LEVEL

The militaries of various countries have generally developed IO doctrine as part of their operational planning (*JWP 3-80*, 2002; *JP 3-13*, 2014; *MC 0422/6 NATO Military Policy for Information Operations*, 2018). Although the specifics vary, most Western militaries view IO as including "military information support operations (MISO), military deception, operations security, public affairs, electronic warfare (EW), civil affairs operations (CAO), and cyberspace" (ATP 3-13.1, 2018). One important distinction between military IO and broader efforts is that, doctrinally, military IO focuses on degrading the decision-making of opposing leaders – whether through electronic or physical disruption or through 'getting inside their heads'

– while broader strategic IO has tended to focus on the populace of opponents (*Field Manual FM 3-13*, 2003; Blackmore, 2003, p 14).

Although military IO has the most developed doctrines and operational concepts, there are issues even at this level. The first is the broadness of the missions subsumed under the title of IO. Actually trying to synchronize and operationalize these disparate skill sets into a coherent mission plan, much less a broader strategy, presents significant difficulties. Likewise, even the term "IO" remains somewhat amorphous: "As a consequence, there is little in the way of standardization across staff sections, offices, organizations, and even individuals. Many of the concepts and terms associated with IO and OIE [Operations in the Information Environment] are viewed as esoteric and are not well understood across the joint force" (Schwille et al., 2020, p 2). Beyond this, there is significant flux in basic military doctrines concerning IO, to the extent that some even have proposed that the term IO be replaced with 'operations in the information environment' (Schwille et al., 2020, p 4). Although continued doctrinal development is, of course, to be encouraged as more sophisticated analysis is conducted, trying to carry out strategic planning when doctrine is ever-changing can be very difficult.

2 THE CRITICALITY OF ANALYSIS

Whether at the operational or strategic level, for the best results a thorough intelligence analysis of the target must be conducted. This consists of three essential components: vulnerability, susceptibility, and accessibility. The vulnerability analysis focuses on who are the most likely to respond to IO efforts; susceptibility focuses on how likely they are to respond to our campaigns; and accessibility tries to maximize efforts to get the message to the intended targets. A similar argument, using a marketing approach, is provided by Jackson (2016). Likewise, Blackmore (2003) suggests using public relations procedures.

Behavioral analysis provides a good system for providing intelligence support to information operations. It should try to answer the following questions:

- What has the actor (individual or group/organization) done in the past?
- What are useful indicators in past behaviors?
- What estimative value does past behavior have?

Assessing social and political trends among segments of the populace in other countries is also critical. This is particularly important if there are existing cleavages that can be taken advantage of. In some cases, these may be evolutionary, consistent over time, or have changed significantly based on particular events. Pattern analysis using observable behaviors can be particularly useful for seeing whether common actions result in similar social or political outcomes. The underlying logic is to identify both psychological and sociological vulnerabilities which could prove susceptible to IO campaigns. As will be noted below, some of the most effective IO campaigns in the past – and likely ongoing – have not relied on “false” information, but rather have leveraged facts in a selective fashion to try to achieve a country’s goals.

The key ingredient in this is knowledge of the analysts. Lt. Gen. Dennis Crall, Director of Command, Control, Communications and Computers/Cyber and Chief Information Officer, Joint Staff, J6 emphasized this point: “Do you understand that environment? Do you speak the native language? Do you speak the number of dialects in that area? Do you understand anthropology, religion, history when it comes to context? Many of our messages that sound righteous to us fail miserably when introduced to very specific populations during different times,” (Magnuson, n.d.). During the same address, he argued that the US is not in a good position with regard to these requirements at the moment; Crall said that there has been a sharp decline in information operations skills in the military. Those who honed their craft at the end of the Cold War have retired: “I’ve said goodbye to them years ago. They’ve gone on to their second careers, and many of them now are gone. We don’t build information experts who have deployed and have experience in areas like we did even a decade ago” (Magnuson, n.d.).

It may also be noted that there are reportedly significant issues with the actual authorities given to both analysts and operators for ‘offensive’ IO measures (Jajko, 2002). To a large extent, this is a result of conflating traditional information operations campaigns with cyber warfare. Most attention in the last number of years has focused on the latter rather than the former (Schmitt and O’Donnell, 1999; Jensen, 2017; Corn, 2021). There still seem to be significant legal and regulatory gaps in the authorities granted on which populations are allowed to be targeted and the types of IO campaigns that are permitted.

3 STRATEGIC INFORMATION OPERATIONS

The discussion thus far has centered on the purely military side of IO. Arguably, IO can have (and has had) more significance at the higher strategic level. At this level – above normal military planning – the overall population of a country is targeted, rather than focusing on elements of the military. The ultimate function of IO seems primarily to create friction between the populace and the government or between segments of the populace. Over time, such efforts can have a corrosive effect on public trust and confidence in its government. Using an analogy from another era of physical sabotage, it is akin to putting sand in the gearbox of a locomotive, rather than blowing it up. Although slower, the results can be similar. Ideally, of course, such a long-term effort will be combined with more focused IO efforts for specific goals. If conducted with effective strategic planning, the larger strategic efforts will complement the more operational approaches: “information activities are strategically aligned with military activity occurring covertly at any point on the spectrum of conflict” (Hammond-Errey, 2019, p 3).

3.1 Most strategic IO has targeted populations

As noted, truly strategic IO has tended to target the populations of opposing countries. In many ways, existing points of friction have been weaponized, rather than inventing fresh 'realities'. Finding these areas of existing contention has been relatively easy, particularly in democratic societies. In fact, some have argued that democratic societies are particularly vulnerable to these efforts (Paterson and Hanley, 2020, p 440). Although the various press and speech freedoms in democratic states make broad IO campaigns easier, the multiple information transmission means now available make true control of all information flows difficult even for highly authoritarian countries.

In the case of the Soviet Union, and seemingly still in the case of Russia, efforts to identify specific segments of the population for targeting seem to be somewhat minimal. IO efforts appeared to focus more on particular themes rather than on sub-groups. As one example, the KGB's campaign to inflame US race relations was described by a senior KGB officer stationed in the United States, Oleg Kalugin, who worked undercover as a Radio Moscow correspondent in New York and Washington in the 1960s and early 1970s: "Our active measures campaign did not discriminate on the basis of race, creed, or color: we went after everybody" (Walton, 2022).

A consequence of the Soviet/Russian approach is that "It is thus not the quality of information that is important in Russian information warfare, but the quantity" (Thornton, 2015, p 46). One reflection of this system has been the Russian Internet Research Agency, which became notorious during the 2016 US presidential election. Studies of its operations indicate a group that valued output with much less concern than effectiveness (Dawson and Innes, 2019; Rid, 2020). At times, in fact, its workers – most of whom were given quotas for producing traffic – transmitted competing positions on IO themes. Although it is possible that these competing positions were intentionally designed to sow friction in the target populations, it is hard to escape the suspicion that in many ways they simply reflected poor internal controls. However well the Russians (and perhaps the Chinese) have succeeded with such 'bulk' campaigns, the resources required for this approach are unlikely to be available to many Western countries.

3.2 'Truth' versus falsehood

Most IO campaigns should be and have been based on at least kernels of truth. Even actual disinformation will be more readily accepted by willing audiences if there are pre-existing cleavages that can be taken advantage of. This has likely gotten easier in today's environment where 'authoritative' news sources – such as the *BBC, London Times, New York Times*, etc. – are less followed by significant numbers of people, who instead are getting their 'news' from various internet sources of dubious reliability. If a disinformation theme tracks with their perceived realities, it will probably be believed.

Despite having themes that are based on these perceptions of reality, there clearly has been some successful use of forgeries. In some cases, the forgeries simply have not been expected to have much credibility. Bittman noted that a Sudeten German leader was targeted by forged letters purportedly written by him asking for financial support from various foreign figures, which he then had to explain (Bittman, 1972, p 13). There seemed to be little expectation that these letters would have a long shelf life before being exposed as forgeries, but simply having to deal with exposing them created a significant distraction. One other issue with forgeries should be noted. Earlier IO campaigns in developing countries suggest that in these types of environments, even egregiously bad forgeries and what typically would be seen as false narratives could have significant implications. A good example of this approach was the Soviet campaign in many African countries in the 1980s blaming the US for the deliberate introduction of the AIDS virus (US Department of State, 1987). Even poor forgeries – and they seemed to be rather common – had potential usefulness: "Most forgeries were released to the public, with the intended victim promptly denying the authenticity, but the KGB calculated that the denial would not entirely offset the public damage" (McCauley, 2016, p 171).

Third party sources can be critical in getting narratives accepted. Ideally, these sources will have significant credibility. In the past, this would have included respected journalists, newspapers, and other media sources. Currently, it might be more important to focus on social media influencers or popular websites. The actual credibility of the initial source reporting might not always be significant as long as the stories are picked up by foreign press that can spread (and preferably amplify) them. McCauley provides a good example of this from the Cold War, using the example of how the Burmese press was used to plant stories which then grew (McCauley, 2016, pp 155-156).

In many cases, existing groups – whether mainstream or radical – can be the best conduits for getting the message disseminated. Bittman noted that in a disinformation campaign in Germany in an effort to discredit the German government as being influenced by Naziism, a false flag operation in the 1960s using Neo-Nazi propaganda had some actual Nazis distributing the material thinking it was authentic (Bittman, 1972, p 3). At the same time, using such radical groups which, in fact, may not support the political goals (not to mention the ideology) of the government using IO can be problematic. In the same campaign to emphasize the "Nazi" leanings of the German government, the KGB instructed the Stasi officers supervising the campaign: "Our comrades must, however, continue to work amongst Nazis with the greatest skill to prevent them from unwittingly helping to strengthen Nazi movements". It ended by warning that "effective countermeasures would have to be taken at the slightest indication that matters were beginning to get out of hand" (Rid, 2020, p 129).

This also can be a problem with the covert IO support of groups that are in general ideological supporters of the goals of the IO-sponsoring country. Perhaps the largest open-source example of this was the Soviet support for various peace movements in Europe during the Cold War: "The difficulty was balancing Kremlin control of the [front] groups while appearing independent in order to attract non-Communist support" (McCauley, 2016, p 88). This certainly applies to campaigns against countries such as Russia; too close a public identification of movements within these countries can easily lead to them being branded as 'foreign agents' and significantly reduce their potential impact.

3.3 What is viewed as public diplomacy by one country can be viewed as disinformation by opponents

A corollary to the previous paragraph is that public support for foreign opposition groups which is too overt can boomerang on the country providing it. This may be particularly critical in ongoing IO campaigns directed by Russia and the US against each other. One aspect of IO and disinformation which is commonly not given sufficient attention by observers is the extent to which other countries view the US and other Western countries as a major user of these techniques. Typically, the US government stresses terms such as public diplomacy and support for democratic trends, but these efforts can begin to look a lot like disinformation to those opponents against whom they are directed. In fact the US has, of course, conducted significant disinformation and clandestine operations in the past, such as the early Cold War operations in East Germany, the early post-World War II Italian elections, and clandestine support for the Solidarity movement in Poland.

This last operation – known as QRHELPFUL – was particularly wide-ranging and reportedly received support (however unwittingly) from US labor unions, the Catholic Church, and some humanitarian organizations. Throughout the operation, despite both suspicions and accusations of the CIA 'running' the Solidarity movement, QRHELPFUL achieved one significant goal: "the CIA wanted to smuggle materials in such a way that Solidarity members never definitively knew the CIA was providing aid. Solidarity's legitimacy would have been severely undermined if there was unequivocal evidence of CIA assistance" (Jones, 2018, p 6).

Such history continues to be germane to the IO conflict between the US and Russia. The so-called Gerasimov Doctrine in fact focuses on defense against US IO operations (Gerasimov, 2016). As a further example of the Russian military's almost-fixation on the possibility of US disinformation:

The main objective of information war is to capture the consciousness of the population of the Russian Federation, to undermine the moral-fighting potential of the armed forces; i.e., to set the stage for political, economic, and military penetration. With this goal in mind, both secret information and psychological operations (actions) are being prepared and continuously conducted, not just by designated state structures of traditional enemies of Russia, but also by its allies and friendly countries (Korotchenko, 1996).

The same source provides several other examples of this argument. This is not to argue for moral equivalency or to suggest that current US IO efforts are in fact as significant as the Russian sources claim (given the issues with the lack of qualified personnel noted earlier); it does however indicate that, for at least the Russian military and almost certainly for the larger Russian security apparatus, the view is that IO is a tit-for-tat conflict. Thomas (1998) provides a detailed examination of the Russian structure for counter-IO operations. As such, expecting a reduction in IO efforts is futile.

3.4 Official reactions to IO campaigns to try to counter them may increase their effectiveness

Counter-IO efforts are virtually inevitable and in fact are necessary. The issue, however, is how well these are planned and implemented. One such effort during the Cold War – the Active Measures Working Group – has typically been used as an example of how counter-IO can be achieved. Among other efforts, the organization provided regular public reports on Soviet propaganda efforts (US Department of State, 1987). In a detailed study, Schoen and Lamb (2012) provided a very positive judgement of the operations of the Active Measures Working Group.

More recently, in 2016, the US State Department established the Global Engagement Center with the mission to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations" (Global Engagement Center, 2024). Others have argued that the counter-IO effort should in fact be even more formalized and strengthened, with the establishment of a full-time multi-agency center akin to the National Center for Counterterrorism (Walton, 2022).

Unfortunately, efforts to counter disinformation can often simply reinforce the IO campaign by giving it increased airtime: "Therefore, debunking false information and refuting provided data as incoherent and leading to false assumptions is ineffective in countering disinformation campaigns. Also, the more the data seems credible despite being disinformation, and the more it is tailored to seduce the opponent's cognitive biases, the more effective it is" (Bagge, 2019, p 37). Perhaps the most prominent example of this issue was the plethora of official US government reports on Russian interference in the 2016 elections and the potential for further interference (Mueller, 2019; National Intelligence Council, 2021). The conclusions of these reports could easily lead to considerable cognitive dissonance among members of the public; at the same time as government officials were stressing the reliability of the election process, they were warning of the extent of Russian interference. It would have been very easy for at least segments of the population to conclude that the government either was not being honest with them about the safety of the electoral process, or that the threat was overstated. Either way, the result could be decreased public trust in the government. Again, the immediate results might not be dramatic, but the corrosive effect could be important over time: "This is because the perception of interference can be just as damaging as actual interference, and thus beneficial to Russia's central aim of creating chaos to erode trust in democracy, and degrade western societal and political legitimacy" (Paterson and Hanley, 2020, p 443).

3.5 Actually measuring the effectiveness of strategic IO campaigns has been virtually impossible

Many approaches for assessing how well IO efforts have worked have been suggested, but no useful metrics have resulted. One review of the available literature concluded that the impact of persuasive campaigns has been limited (Wallenius, 2022). Likewise, another study concluded that "Contrary to past and present claims about foreign malign "hidden hands" in U.S. domestic affairs, in fact the Soviet Union's disinformation strategy, and its impact, were limited: it targeted and amplified existing divisions within American society, doing nothing more than magnifying them" (Walton, 2022).

Even at the operational level, the actual impact of IO, at this level probably better viewed as propaganda, has been difficult to quantify. At their simplest (and perhaps simplistic), tactical efforts have been measured by the number of enemy troops surrendering who present surrender chits[1] or the like. Clearly, there is no simple one-to-one relationship between a tactical IO campaign and troops wanting to give up the fight. In many instances, even in such 'simple' environments, the efficacy of a particular campaign remains unknown until after it is over. Also, of course, what might work well at a particular point in time or in a particular environment may be ineffective or even counterproductive in a different time or environment. Some measurement tools may be useful at lower levels in relatively benign environments, such as peacekeeping missions; one approach that has been suggested is the use of corporate public relations measurement techniques (Blackmore, 2003).

Conclusion

In the United States, some proposals have been put forth that because the Defense Department already has some authorities for IO, it should be the proponent for all national IO policies and operations (Hatch, 2019, pp 73-85). How well other government agencies would view this approach – particularly for the 'darker shades' of IO – is questionable. More broadly, most Western countries would likely view such organizational structures as not being conducive to appropriate civil-military relations. Nevertheless, military strategists must take into account the broader strands of strategic IO in their strategic planning.

Most Western countries have focused on defensive measures against IO campaigns conducted against them. As noted, this may be counterproductive in many cases, and more broadly, may in fact be a poor strategic decision. Ceding the initiative to an opponent is unlikely to ever succeed in the strategic longer term. Certainly,

[1] *Highly visible sheets of paper distributed among enemy troops which promise safe conduct and good treatment for those who surrender*

efforts to counter disinformation will remain necessary, but a case-by-case approach will never provide a coherent counter campaign. Understanding previous patterns and strategic approaches are required both for defensive and possible offensive information operations campaigns.

References

1. *Babbage, R., 2019. Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail. 2 vols. Washington DC: Center for Strategic and Budgetary Assessments.*
2. *Bittman, L., 1972. The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare. [1st ed. Syracuse, N.Y.]: Syracuse University Research Corp.*
3. *Blackmore, T. R., 2003. Assess the Importance of Measures of Effectiveness (MOE) for the Further Development of UK Information Operations. Defence Studies 3(3), September 2003, pp 9–37. https://doi.org/10.1080/14702430308405075 (Accessed 17 January 2024).*
4. *Dawson, A., and Innes, M., 2019. How Russia's Internet Research Agency Built Its Disinformation Campaign. The Political Quarterly 90(2), June 2019, pp 245–256. https://doi.org/10.1111/1467-923X.12690. (Accessed 17 January 2024).*
5. *Dowse, A., and Dov Bachmann, S., 2022. Information Warfare: Methods to Counter Disinformation. Defense & Security Analysis 38(4), October 2, 2022, pp 453–469. https://doi.org/10.1080/14751798.2022.2117285. (Accessed 17 January 2024).*
6. *Gerasimov, V., 2016. The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Translated and Reprinted in Military Review, February 2016, pp 23–29.*
7. *Global Engagement Center, 2024. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (Accessed 17 January 2024).*
8. *Hammond-Errey, M. 2019. Understanding and Assessing Information Influence and Foreign Interference. Journal of Information Warfare 18(1), Winter 2019, pp 1–22.*
9. *Hatch, B., 2019. The Future of Strategic Information and Cyber-Enabled Information Operations. Journal of Strategic Security 12(4), January 2019, pp 69–89. https://doi.org/10.5038/1944-0472.12.4.1735 (Accessed 17 January 2024).*
10. *Headquarters, Department of the Army, 2003. Field Manual FM 3-13.*
11. *Headquarters, Department of the Army, 2018. ATP 3-13.1. The Conduct of Information Operations.*
12. *Jackson, C. F., 2016. Information Is Not a Weapons System. Journal of Strategic Studies 39(5-6), September 18, 2016, pp 820–46. https://doi.org/10.1080/01402390.2016.1139496 (Accessed 17 January 2024).*
13. *Jajko, W. A., 2002. Critical Commentary on the Department of Defense Authorities for Information Operations. Comparative Strategy 21(2), April 2002, pp 107–14. https://doi.org/10.1080/01495930290043074 (Accessed 17 January 2024).*
14. *Jones, S. G., 2018. Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare. Washington DC: CSIS Brief.*
15. *Jones, S., 2018. Combating Information Operations: Developing an Operating Concept. Cambridge, MA: Harvard Belfer Center.*
16. *Klein, H., 2018. INFORMATION WARFARE AND INFORMATION OPERATIONS: RUSSIAN AND U.S. PERSPECTIVES. Journal of International Affairs 71(1.5), pp 135–142.*
17. *Korotchenko, E. G., 1996. Informatsionno- Psikhologicheskoye Protivoborstvo v Sovremennykh Usloviyakhn [Information - Psychological Confrontation under Modern Conditions]." Voennoye Mysl [Military Thought], February 1996, pp 19–26.*

18. *Magnuson, S., 2022. US Still Playing Catch Up in Information Operations. National Defense Magazine, February 11, 2022. https://www.nationaldefensemagazine.org/articles/2022/2/11/still-playing-catch-up-in-information-operations (Accessed 17 January 2024).*
19. *Ministry of Defence, 2002. Joint Warfare Publication 3-80 Information Operations. Swindon, UK: The Joint Doctrine & Concepts Centre, Ministry of Defence.*
20. *Mueller, R., 2019. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Washington DC: Department of Justice, March 2019.*
21. *National Intelligence Council, 2021. Foreign Threats to the 2020 US Federal Elections. Washington DC, March 10, 2021.*
22. *NATO, 2018. MC 0422/6 NATO Military Policy for Information Operations. Brussels.*
23. *Polyakova, A., and Boyer, S. P., 2018. The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition. Washington DC: The Brookings Institution.*
24. *Rid, T., 2020. Active Measures: The Secret History of Disinformation and Political Warfare. First edition. New York: Farrar, Straus and Giroux.*
25. *Schoen, F., and Lamb, C. J., 2012. Strategic Perspectives 11: Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. Washington DC: National Defense University.*
26. *Schwille, M., Atler, A., Welch, J., Paul, C., and Baffa, R. C., 2020. Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities between Intelligence and Information Professionals. Santa Monica, CA: RAND.*
27. *Sieting, L. A., 2003. Intelligence Support to Information Operations: Today and in the Objective Force. Military Intelligence, September 2003, pp 56–60.*
28. *Thomas, T. I., 1998. Russia's Information Warfare Structure: Understanding the Roles of the Security Council, Fapsi, the State Technical Commission and the Military. European Security 7(1), March 1998, pp 156–172. https://doi.org/10.1080/09662839808407354 (Accessed 17 January 2024).*
29. *Thomas, T. L., 1997. Russian Information-Psychological Actions: Implications for U.S. PSYOP. Special Warfare 10(1), Winter 1997, pp 12–19.*
30. *Thornton, R., 2015., The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. The RUSI Journal 160(4), July 4, 2015, pp 40–48. https://doi.org/10.1080/03071847.2015.1079047 (Accessed 17 January 2024).*
31. *United States Department of Defense, 2014. Joint Publication 3-13 Information Operations. Washington DC: Department of Defense.*
32. *United States Department of State, 1987. "Soviet Influence Activities: A Report of Active Measures and Propaganda, 1986-1987," August 1987.*
33. *United States Department of State, 1987. Soviet Influence Activities: A Report of Active Measures and Propaganda, 1986-1987. Washington DC: United States Department of State.*
34. *United States Department of State, 2024. "Global Engagement Center 'Mission & Vision,'" January 17, 2024. https://www.state.gov/bureaus-offices/under-secretary-for-public--diplomacy-and-public-affairs/global-engagement-center/ (Accessed 17 January 2024).*
35. *Wallenius, C., 2022. Do Hostile Information Operations Really Have the Intended Effects? A Literature Review. Journal of Information Warfare 21(2), Spring 2022, pp 21–35.*
36. *Walton, C., 2022. Old Is New Again: Cold War Lessons for Countering Disinformation. Texas National Security Review, Fall 2022. N. d.*

email: **lawcline@gmail.com**

ORCID: 0000-0002-6174-325X