

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

EDIA

International Journal of Innovative Research in SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462

6381 907 438

 \bigcirc



e-ISSN: 2319-8753, p-ISSN: 2347-6710 www.ijirset.com | Impact Factor: 7.569



Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

HYBRID WARFARE

Dr. Surendra Kumar Pandey

Associate Professor and Head, Department of Defence and Strategic Studies, Acharya Narendra Deo Kisan PG

College, Babhnan, Gonda, Uttar Pradesh, India

Abstract: Hybrid warfare is a theory of military strategy, first proposed by Frank Hoffman, which employs political warfare and blends conventional warfare, irregular warfare and cyberwarfare with other influencing methods, such as fake news, diplomacy, lawfare and foreign electoral intervention. By combining kinetic operations with subversive efforts, the aggressor intends to avoid attribution or retribution. Hybrid warfare can be used to describe the flexible and complex dynamics of the battlespace requiring a highly adaptable and resilient response. Hybrid warfare is an emerging, but ill-defined notion in conflict studies. It refers to the use of unconventional methods as part of a multi-domain warfighting approach. These methods aim to disrupt and disable an opponent's actions without engaging in open hostilities.

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

KEYWORDS: hybrid, warfare, military, concept, strategy, methods, weapons

I. INTRODUCTION

Hybrid warfare is warfare with the following aspects:

A non-standard, complex, and fluid adversary. A hybrid adversary can be state or non-state. For example, in the Israel–Hezbollah War of 2006 and the Syrian Civil War, the main adversaries are non-state entities within the state system.



The non-state actors can act as proxies for countries but have independent agendas as well. For example, Iran is a sponsor of Hezbollah, but it was Hezbollah's, not Iran's, agenda that resulted in the kidnapping of Israeli troops that led to the Israel–Hezbollah War. On the other hand, Russian involvement in Ukraine can be described as a traditional state actor waging a hybrid war (in addition to using a local hybrid proxy) although Russia denies involvement in the Ukraine conflict. A hybrid adversary uses a combination of conventional and irregular methods. Methods and tactics may include conventional capabilities, irregular tactics, irregular formations, diplomacy, politics, terrorist acts, indiscriminate violence, and criminal activity. A hybrid adversary may also use clandestine actions to avoid attribution

入 う は IJIRSET | e-ISSN: 2319-8753, p-ISSN: 2347-6710| <u>www.ijirset.com</u> | Impact Factor: 7.569|

Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

or retribution. The methods are used simultaneously across the spectrum of conflict with a unified strategy. A current example is the Islamic State's transnational aspirations, blended tactics, structured formations, and cruel use of terrorism as part of its arsenal.[1]



A hybrid adversary is flexible and adapts quickly. For example, the Islamic State's response to the US aerial bombing campaign was a quick reduction of the use of checkpoints, of large convoys, and of cellphones. Militants also dispersed among the civilian population. Civilian collateral damage from airstrikes can be used as an effective recruiting tool.

A hybrid adversary uses advanced weapons systems and other disruptive technologies. Such weapons can be now bought at bargain prices. Moreover, other novel technologies are being adapted to the battlefield such as cellular networks. In 2006 Hezbollah was armed with high-tech weaponry, such as precision guided missiles, which nation-states typically use. Hezbollah forces shot down Israeli helicopters, severely damaged a patrol boat with a cruise missile, and destroyed heavily-armored tanks by firing guided missiles from hidden bunkers. It also used aerial drones to gather intelligence, communicated with encrypted cellphones, and watched Israeli troop movements with thermal night-vision equipment.[2]

Use of mass communication for propaganda. The growth of mass communication networks offers powerful propaganda and recruiting tools. The use of fake-news websites to spread false stories is a possible element of hybrid warfare.

A hybrid war takes place on three distinct battlefields. They are the conventional battlefield, the indigenous population of the conflict zone, and the international community.

II. OBSERVATIONS

Washington and Moscow are engaged in a war of words over a spate of ransomware attacks against organisations and businesses in the US and other countries. These increasingly sophisticated cyber-attacks represent a new type of warfare aimed at disorganising and even destroying a nation's economy. The scale of cyber-attacks conducted at a military level signals the involvement of state actors behind the scenes to organise or encourage these attacks. Russia has emerged as one of the international actors that has developed a sophisticated cyberwarfare strategy.

e-ISSN: 2319-8753, p-ISSN: 2347-6710 www.ijirset.com | Impact Factor: 7.569



|| Volume 10, Issue 12, December 2021 ||

DOI:10.15680/IJIRSET.2021.1012080



So what do we know about the way Russia pursues hybrid warfare via cyber-attacks? Russia's cyberwarfare doctrine, or "gibridnaya voyna" (hybrid war), was shaped by political scientists such as Alexandr Dugin – a Russian philosopher dubbed"Putin's Rasputin" or "Putin's brain". He is also a sociology professor at Moscow State University and was targeted by US sanctions following Russia's takeover of Crimea in 2014.[3]

Another key thinker in this area is Igor Panarin, a senior adviser to Putin with a PhD in psychology. Senior military figures include Valery Gerasimov, chief of Russia's general staff and the author of the "Gerasimov Doctrine", which, according to the Carnegie Foundation, is "a whole of government concept that fuses hard and soft power across many domains and transcends boundaries between peace- and wartime".

III. DISCUSSION

In hybrid warfare the state responsible for the actions will often use non-state actors, which allows it to deny responsibility. Washington and Moscow are engaged in a war of words over a spate of ransomware attacks against organisations and businesses in the US and other countries. These increasingly sophisticated cyber-attacks represent a new type of warfare aimed at disorganising and even destroying a nation's economy.

This has been called "hybrid warfare". It's a mixture of conventional and unconventional methods used against a much stronger adversary that aims to achieve political objectives that would not be possible with traditional warfare.[4]



よう総 IJIRSET | e-ISSN: 2319-8753, p-ISSN: 2347-6710| <u>www.ijirset.com</u> | Impact Factor: 7.569|

Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

The problem is often identifying the culprits. In hybrid warfare the state responsible for the actions will often use nonstate actors, which allows it to deny responsibility. But over the past two decades, many cyber-attacks targeting western state institutions and businesses have been far more sophisticated than a couple of tech-savvy individuals operating as "lone wolves" and bear the hallmarks of actions taken with the support or approval of a hostile government.

The scale of cyber-attacks conducted at a military level signals the involvement of state actors behind the scenes to organise or encourage these attacks. Russia has emerged as one of the international actors that has developed a sophisticated cyberwarfare strategy.

So, what do we know about the way Russia pursues hybrid warfare via cyber-attacks? Russia's cyberwarfare doctrine, or "gibridnaya voyna" (hybrid war), was shaped by political scientists such as Alexandr Dugin – a Russian philosopher dubbed Putin's Rasputin or Putin's brain. He is also a sociology professor at Moscow State University and was targeted by US sanctions following Russia's takeover of Crimea in 2014.

Examples of "hybrid war"	
 Russia (vs Ukraine) Russia (vs Georgia) AQ, ISIS (vs West) Hamas (vs Israel) Iran (vs GCC) etc. 	 Allies (vs Axis) UK (vs IRA) Canada (vs South Africa) US, GCC (vs Syria) US (vs Nicaragua) Coalition (vs Libya) etc.

Cyberspace is often shown as having a physical layer (hardware), a logical layer (how and where the data is distributed and processed) and a human layer (users). Mostly it is managed by private organisations rather than state actors. So cyber-attacks are in a grey area when it comes to who should be responsible for prevention. There is also the question of who is mounting the attacks and whether they are criminal enterprises or backed by a state agency.

This confusion for the responsibility to protect plays in the hands of the Russian government. It can hurt its adversaries, no matter how large or strong, without having to wage a military campaign.

In recent years, cyber-attacks perpetrated by Russian crime groups have targeted hospitals, energy grids and industrial facilities. The Kremlin has described allegations of its involvement as "groundless". But even though there might not be a direct connection between the government and whoever is mounting the attacks, Russia knowingly allows these groups to operate from its territory.[5]

Russia's state agencies have offered their services in tracking down these criminal groups. But this is a familiar pledge over the years and nothing has come of it - something that is thrown into sharp relief when compared with their



| e-ISSN: 2319-8753, p-ISSN: 2347-6710| <u>www.ijirset.com</u> | Impact Factor: 7.569|

Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

enthusiasm to tackle activist groups operating domestically. Many countries have intensified their efforts to develop strategies to counter cybercrime. These initiatives include hybrid warfare defence exercises in 24 EU member states, wargaming an orchestrated cyber-attack against EU military and cybersecurity infrastructure.

The EU has also established what it calls a "hybrid fusion cell" to provide strategic analysis to EU decision-makers in its bid to deter and respond to cyber-attacks.



The group of analysts within the EU Intelligence and Situation Centre (EU Intcen) is analysing intelligence coming from the EU and various national institutions such as the GCHQ, MI5 and police intelligence agencies in the UK and providing a risk assessment for policymakers to shape their domestic policy.

Both the EU and the US have imposed sanctions on Russian individuals and entities for their harmful activities targeting cyber infrastructure. But tackling such a threat from tightly disciplined and rigidly hierarchical state-sponsored groups is not easy.

As fast as western intelligence can develop new initiatives to tackle hybrid tactics, cybercriminals seem able to develop new means of attack. So an agile governance model is needed to efficiently use public and private resources to tackle the threat from hybrid warfare threat.

The EUCTER network, led by the International Centre for Policing and Security at the University of South Wales with 13 partners across Europe and Israel is developing a range of innovative models that you can read about in detail on our website.

Hybrid warfare is a vast, complex and fast-moving threat – which requires a proportionate response if nations are going to defend themselves against.[6]

IV. RESULTS

Hybrid warfare combines military and nonmilitary as well as covert and overt means, such as disinformation, cyberattacks, economic coercion, lawfare, corruption, and irregular and regular forces. Hybrid methods are used to blur the lines between war and peace. They attempt to undermine target institutions and populations to achieve strategic aims. While these threats are not new, technological advancements and increasing global connectivity have recently expanded their speed, intensity, and scope. To more effectively tackle future hybrid threats from Russia, China, and non-state actors, the transatlantic community and NATO should improve in the following key areas.[7]



Raise public awareness of hybrid threats. To counter hybrid threats, the transatlantic community must first understand what they are. Participants in the digital campaign considered disinformation and cyberwarfare to be the most common and pressing hybrid threats of today. On the other hand, there was less awareness of economic coercion, political subversion, and lawfare. Experts noted that while the existence of these threats is acknowledged individually, their use in conjunction makes them increasingly disruptive and their interconnectivity is underexplored. There is an urgent need to understand the impact of these threats on transatlantic societies and institutions and which hybrid actions are most likely to succeed or cause damage to allies in the future. Future hybrid threats that require more attention include weaponized corruption, automated armies, and biowarfare. 80% of respondents to a campaign poll believed NATO's 2021 Brussels Summit Communiqué adequately prioritized hybrid threats.

Increase NATO's speed of recognizing hybrid threats. Looking to the future, participants agreed the Alliance must be able to more quickly recognize and respond to hybrid campaigns before they can fully unfold and achieve their aims. This requires investing more in intelligence, surveillance, and reconnaissance capabilities; leveraging open-source information; and utilizing human-machine teaming to compete with adversaries that have more centralized, rapid decision-making than NATO. These capabilities can aid in the attribution of hybrid actions to their perpetrators, which are purposefully difficult to detect. To help the Alliance better recognize, conceptualize, and plan for hybrid threats, campaign participants suggested NATO consider a sixth "cognitive" or "human" domain of future warfare.[8]

Get comfortable operating more proactively below the threshold of conflict. Hybrid threats often fall below NATO's Article 5 threshold of armed attack laid out in its founding treaty. This makes it difficult for NATO member states to respond swiftly and appropriately in collective defense. NATO has already acknowledged that a serious cyberattack can trigger Article 5. But rather than waiting for today's ongoing cyberattacks to escalate to that level, 93% of survey respondents agreed NATO must play a more proactive role in addressing below-threshold hybrid threats. For example, NATO could help coordinate more active and persistent cyber defense capabilities from nations, such as "hunt forward" teams. Under Article 3 of its founding treaty, NATO can also help nations mitigate the effects of hybrid threats by setting resilience standards and capability targets.



Build trust between governments, institutions, and publics. Survey respondents overwhelmingly agreed that national governments bear the most responsibility for countering hybrid threats. But their trust in officials and institutions to take such action varied greatly, with nearly 50% of respondents rating their trust levels at three on a five-point scale. This lack of confidence plays directly into the aims of adversaries' hybrid campaigns, inhibits societal resilience, and undermines government response. NATO ally and partner publics should engage in more civil education campaigns and trust-building exercises to strengthen democracies against hybrid threats.[9]

Boost public-private cooperation against hybrid threats. Experts highlighted that the private sector often owns or operates much of the critical infrastructure that is targeted by hybrid warfare — from energy pipelines to electric grids to online platforms. To spot and stem future hybrid threats, a majority of participants agreed that governments, militaries, and security institutions such as NATO must work more closely with the private sector to develop indications and warning systems, response protocols, and resilience and threat mitigation measures against hybrid warfare. Governments should also engage to provide legal parameters and budgetary incentives for private sector compliance.[10]

V. CONCLUSION

NATO's success as a collective defense organization lies in its ability to rally twenty-nine member states in defense of any one of them. Cohesion is what makes the alliance strong and unique, but it is difficult to sustain day after day, under constant pressure from adversaries.

One useful way to measure cohesion is in financial terms. Despite a pledge to contribute the equivalent of at least 2 percent of their gross domestic product to defense by 2024, some member states seem likely to miss the target. While this does not prove that the allies disagree on the nature and gravity of the threats before them, it does strongly suggest that some have not fully bought into the agreed priorities.

e-ISSN: 2319-8753, p-ISSN: 2347-6710 www.ijirset.com | Impact Factor: 7.569



Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080



Many factors are undermining cohesion in NATO. In an era with no single unifying threat, different members inevitably have different interests in diverse centers of power and influence. Allies also diverge on what constitute democratic standards and appropriate responses to competition with non-Western actors[11]

It is up to individual countries to safeguard their freedom to respond to a call for help from an ally, address vulnerabilities and gaps in their national systems, and take proactive measures to reduce risks. But the alliance as an organization can help. This is especially true when it comes to understanding and responding to new threats to cohesion. None is more relevant than the hybrid war for hearts and minds that NATO's adversaries are waging through political interference and disinformation.

While not a new phenomenon, hybrid warfare has been widely mentioned in international discourse since at least 2014. The Russian military intervention in Ukraine and annexation of Crimea showed that NATO and its member states lacked readymade responses to the emergence of a threat aimed directly at solidarity and cohesion. The experience has prompted allies to rethink, act, and adapt quickly, especially with regard to instruments for protection beyond triggering Article 5 of NATO's founding treaty, which declares that an attack on one ally is an attack on all.[12]

Hybrid warfare includes a variety of activities and covers the use of different instruments to destabilize a society by influencing its decisionmaking. Frequent instruments include:

• Interference in electoral processes: An adversary can use techniques from campaigning through the media and social networks to securing financial resources for a political group to influence the outcome of an election in a direction that favors the adversary's political interests.

• Disinformation and false news: An adversary can create a parallel reality and use falsehoods to fuel social fragmentation. The idea is to disorient the public and make it difficult for a government to seek public approval for a given NATO policy or operation.



入 う は IJIRSET | e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569

Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

- Cyber attacks: An adversary can pressure NATO governments into not coming to each other's aid in times of crisis by threatening devastating cyber attacks aimed at the civilian population. Examples include attacks on networks governing hospitals or electricity and water supplies.
- Drone attacks: These are similar to cyber attacks but on a more limited scale. An adversary can use remotely piloted platforms to inflict misery on civilians by crippling the operations of airports, air ambulances, and police helicopters. Such attacks can also hamper military airspace operations in early phases of a conflict.
- Financial influence: An adversary can make investments, conclude unfavorable energy-supply deals, or offer loans that make a country vulnerable in the long run to political pressure.

Russia is the most frequently cited source of hybrid attacks, particularly disinformation, interference in elections, and cyber attacks. It and other states often act via third, nonstate entities such as nationalist, criminal, or terrorist groups. This leaves the attacking state room for deniability, confuses the attacked country, and can prevent a timely and adequate response. Most hybrid operations to date have featured a mixture of mechanisms used by state and nonstate actors, and a clear line between them is difficult to draw.

NATO's efforts to address hybrid threats have been conducted at two levels: defining strategy at the supranational level and assisting the target countries at the national level. The latter effort will receive a boost when the new counterhybrid support teams on which members agreed in July 2018 fully come into effect. NATO's Joint Intelligence and Security Division is in charge of hybrid-related research and analysis, while the Public Diplomacy Division tracks disinformation through online instruments. The Emerging Security Challenges Working Group, established in 2012, has a goal to identify and prioritize nontraditional threats.[13]

Because hybrid attacks are a threat to the West as a whole, not just NATO, and because they mostly rely on nonmilitary tools, the alliance has been strengthening its cooperation with the European Union (EU). One useful tool available to both organizations is the joint European Center of Excellence for Countering Hybrid Threats, established in Helsinki in April 2017.

VI. PREVENTIONS AND RECOMMENDATIONS

Build resilience by fostering democracy

The first, self-evident recommendation is to deny adversaries the opportunities they exploit for hybrid attacks. The more stable the political systems and economies of NATO countries are, the less suitable ground they represent for hybrid threats. A government that is credible, popular, and trusted will have an easier time winning support for its chosen course of action in NATO than other governments and will be better able to resist disinformation and other forms of interference and blackmail.

Military-Centric Warfare Center of Gravity: focused on military decision

Center of Gavity

J.Schmid

Hierarchical Structure

Hybrid Warfare

Center of Gravity: focused on broad spectrum of civil & military domains



Non-hierarchical / dynamic /flexible Structure Multiple and shifting Centers of Gravity

よう 🖄 IJIRSET | e-ISSN: 2319-8753, p-ISSN: 2347-6710| <u>www.ijirset.com</u> | Impact Factor: 7.569|

Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

Western Balkan countries seem particularly vulnerable, as their citizens tend to have low trust in the authorities and do not believe that their judiciaries are truly independent. In opinion polls, as many as 70 percent of respondents said that the law did not equally apply to all. Democracy and trust have declined in most Western Balkan countries over the last ten years, a trend that overlaps with the crisis of democracy throughout Europe.

Steps that strengthen democracy and economies are the most effective way of building resilience against hybrid attacks. Corruption deserves particular attention. Not all authoritarian and illiberal governments are corrupt, but most abuse access to public and European funds to give themselves a competitive advantage over political rivals.



shutterstock.com · 2079402004

Once on a corrupt path, authoritarians are, in essence, condemned to always seek to remain in power, lest they be prosecuted. It is a vicious circle, and this dynamic between authoritarianism and corruption is not always understood—including by the U.S. and EU leaderships, which does not serve the alliance well.

NATO has few tools to defend democracy and combat corruption among its member states, but allies can do more even within this limited framework. Perhaps an annual report on the rule of law in member states, modeled on the one proposed in the EU, could help. NATO could also highlight good and bad practices in member states on an annual basis and could link serious violations of the law to the suspension of certain political rights. The pressure to comply with democratic standards must exist both before and after a state joins the organization. Naturally, the alliance should continue to help foster democracy in countries that aspire to EU and NATO membership.[12]

Share Best Practices

NATO provides a platform from which allies can work when coping with individual problems and vulnerabilities. The alliance can also help identify particular challenges, sometimes before the governments concerned do, and can play a role in early warning. This matters because rapid decisionmaking is sometimes the key to success in hybrid warfare.

Think and speak coherently

NATO is meeting the hybrid challenge with twenty-nine member states experiencing very different sociopolitical realities and often using different concepts. A unified vocabulary and strategy would limit the misunderstanding of threats, improve collaboration, and make the sharing of lessons learned more effective—so would an agreement on the prioritization of tasks and responsibilities and a shared understanding of NATO's role.

This would greatly help individual countries to build compatible and comparable national strategies. Many of these strategies, including that of the youngest member Montenegro, are in early stages of preparation, but divergences are already becoming evident. Those that have been completed—such as Slovenia's 2018 regulation on cyber and information security or Croatia's 2017 National Security Strategy, which partly deals with hybrid challenges—have largely opted for different approaches.

e-ISSN: 2319-8753, p-ISSN: 2347-6710 www.ijirset.com | Impact Factor: 7.569



Volume 10, Issue 12, December 2021

DOI:10.15680/LJIRSET.2021.1012080



NATO member states must send a unified message inside and out. As strategic communication is a mind-set, it has to be built together carefully and fundamentally.¹² NATO's communication strategy should be a result of joint efforts and hence a common instrument against all threats, not just hybrid ones, at all levels.[10] **Unite forces**

Hybrid threats work across military and civilian domains and therefore require intersectoral, regional, and international cooperation. For NATO, cooperation with the EU is essential given the overlap in the two organizations' memberships and their distinct and complementary responsibilities.

This is understood in theory and reflected in joint declarations, but the practice lags behind. The EU and NATO should adopt a common hybrid strategy. They should also build joint response teams, improve day-to-day coordination, and expand the geographic scope of myth-busting websites such as EUvsDisinfo.eu.

Include Civil Society

The capabilities of think tanks or media groups to detect and defend against hybrid threats often surpass those of governments. Specialized private websites such as Stopfake.org do a better job at recognizing disinformation than many public agencies and often relieve governments of the need to build their own capacities. However, few private initiatives exist.[11]

It is in NATO countries' interest to systematically build private capacity by providing grants through the alliance and other international entities dealing with security issues. Financial support should also cover analysis, not just public diplomacy. The more NATO and individual allies succeed in building a network of experts, the more they strengthen their resistance to hybrid challenges.

Invest in journalism to raise media literacy

Social networks, as currently managed and regulated, lend themselves too easily to the dissemination of disinformation. Regulation falls outside NATO's competence, but the alliance should make known its preference for sensible legislation that makes social networks more impervious to abuse by improving recognition of false profiles and strengthening penalties for hate speech.

Ultimately, the best tool for fighting disinformation is professional journalism. In particular, both NATO and its member states should invest more in investigative journalism to offer high-quality alternatives to false news.[12]

e-ISSN: 2319-8753, p-ISSN: 2347-6710 www.ijirset.com | Impact Factor: 7.569



Volume 10, Issue 12, December 2021

DOI:10.15680/IJIRSET.2021.1012080

Research shows that 70 percent of uses of the term "hybrid threats" by the media are inaccurate. NATO would benefit from helping strengthen journalists' capacity to properly cover and monitor this issue. Well-educated media are an indispensable partner in building social awareness and educating citizens on how to cope with various forms of hybrid pressures. NATO can help by providing training and leading campaigns that improve awareness of hybrid challenges and thus boost local media capabilities in this area.[13]

REFERENCES

1) Nicholas Burns, Douglas Lute, and Seth Johnston, "NATO at Seventy: An Alliance in Crisis," Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2019, https://www.belfercenter.org/publication/nato-seventy-alliance-crisis.

2) Frank Bekkers, Rick Meessen, and Deborah Lasche, "Hybrid Conflicts: The New Normal," TNO Innovation for Life, December 2018.

3)Luigi Del Bene, "Hybrid Impact on the Air Domain," in "Joint Air & Space Conference: The Role of Joint Air Power in NATO Deterrence," Joint Air Power Conference Center, October 2017, https://www.japcc.org/hybrid-impact-on-the-air-domain/.

4) Moscow's intention to use hybrid methods is articulated in several documents—the most recent being the 2014 Military Doctrine, the 2015 National Security Strategy, and the 2015 Information Security Doctrine.

5)"NATO's Response to Hybrid Threats," NATO, July 17, 2018, https://www.nato.int/cps/en/natohq/topics_156338.htm.

6) Luke Coffey, "How to Defeat Hybrid Warfare Before It Starts," Heritage Foundation, January 2019, https://www.heritage.org/defense/commentary/how-defeat-hybrid-warfare-it-starts.

7) "Balkan Barometer 2019: Public Opinion Survey," Regional Cooperation Council, July 2019, https://www.rcc.int/pubs/89/balkan-barometer-2019-public-opinion-survey.

8) In this survey of 180 countries, Albania ranked 99, North Macedonia and Kosovo joint 93, Bosnia and Herzegovina 89, Serbia 87, and Montenegro 67. "Corruption Perception Index 2018," Transparency International, 2019, https://www.transparency.org/cpi2018.

9) Selam Gebrekidan, Matt Apuzzo, and Benjamin Novak, "The Money Farmers: How Oligarchs and Populists Milk the E.U. for Millions," New York Times, November 3, 2019, https://www.nytimes.com/2019/11/03/world/europe/eu-farm-subsidy-hungary.html.

10) Andrew Rettman, "EU Proposes Yearly Rule of Law 'Reports," EUobserver, July 17, 2019, https://euobserver.com/justice/145487.

11) Burns et al., "NATO at Seventy."

12)"Hybrid Threats: A Strategic Communications Perspective," NATO Strategic Communications Center of Excellence, April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

13) Murat Caliskan and Paul-Alexander Cramers, "What Do You Mean by 'Hybrid Warfare'? A Content Analysis on the Media Coverage of Hybrid Warfare Concept," December 2018, https://www.researchgate.net/publication/329782285_What_Do_You_Mean_by_Hybrid_Warfare_A_Content_A nalysis_on_the_Media_Coverage_of_Hybrid_Warfare_Concept/link/5c1a52d392851c22a336ce0a/download.





Impact Factor: 7.569





INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY





www.ijirset.com