World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

CYBERSPACE AND ITS IMPACT ON THE GROWING GEOPOLITICAL POWER OF RUSSIA DURING THE ERA OF VLADIMIR PUTIN: A GEOPOLITICAL VISION

Dr. Ahmed Hassan Mejoul Al-Hasnawi
College of Arts / University of Al-Muthanna, Iraq
E-mail : ahmed.alhasnawi@mu.edu.iq

Article history:
Received: 6th March 2022
Accepted: 8th April 2022
Published: 28th May 2022

Abstract:
Cyberspace is a new field of warfare in the modern era, as countries today urgently need to adapt to new technological threats, and they need to provide information to protect their sovereignty and develop their national strength, and policy makers need to understand the emerging climate of war and deal with it cautiously in light of the impact of the geographical field The political is how power and cyberspace interact. This relationship can be determined through the territories that they can control. Countries have access to new means of attack and espionage through the Internet, and these systems were not previously available in the context of achieving geopolitical sovereignty.
Russian cyber-attacks on military and civilian infrastructure in the West, and the world as a whole, have become an ongoing challenge. This apparent shift in Russian foreign policy has re-emerged Russia as a great power and a powerful player on the international scene, with great capabilities to project geopolitical power that has been greatly amplified, which is a natural consequence. The behavior of the Kremlin developed during the era of President Vladimir Putin and its continuous demand for a distinct area around Russia's immediate periphery, as well as its refusal to accept the security system after the Cold War in Europe, these developments showed Russia's tendency to face risks above its weight along with its improved capabilities in various fields. This research is to shed light on the Russian cyber capabilities, and to answer the following questions: What is Russian cyberspace? What is its role in the growing geopolitical power of Russia? What is Putin's strategy in Russian cyberspace? What are the Russian cyber operations against the adversary countries, and what is Russia's strategy in the cyber field in the future? These questions will be answered within the specified space for this research.

Keywords: Cyberspace, Russia, Geopolitical Power, Vladimir Putin.

1- INTRODUCTION:

Cyberspace today constitutes a new arena for policy makers to deal with, which cannot be separated from geopolitics. Rather, cyber measures must be placed within geopolitics to better formulate and understand cyber threats and develop strategies that enable countries to deal with the physical and virtual aspects of cyber threats. Cyberspace has become a subject of competition for power between stakeholders, a scene of confrontation and a very powerful tool in geopolitical conflicts. Conflicts in or within cyberspace cannot be separated from traditional geopolitical power struggles. geopolitical risks involved in the massive expansion of information and communication systems around the world, and information control has become critical; Because the ability to collect, analyze and process information can provide a strategic advantage for the state and raise doubts on the reliability of others' information, and cyber-attacks can directly disrupt communications, confuse the enemy and affect its operational capabilities that depend on internet networks. In fact, cyber attacks have become one of the deterrence strategies. defense of borders; Because it is difficult to determine the source of these attacks with limited capabilities, and often

Defining Russia's modern approach to war is crucial. This is in order to understand its strategy in cyberspace and cyber security because its view on cyber security is intertwined with its evolving understanding of the nature of war. Its technical

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

repercussions on citizens and on global peace and security appear in the future.
This research sheds light on how Russia employs its cyber capabilities in countries that believe that they constitute a threat to their sovereignty and national security and limit the increase in its global status, as well as revealing the role of cyberspace in the development of Russia's cyber operations and its impact on the growth of its geopolitical power, in addition to revealing some Its cyber activities targeting adversary countries.

2- THE CONCEPT OF CYBERSPACE AND ITS COMPONENTS:

2.1- The concept of cyberspace:

The term cyberspace first appeared in 1984 at NeuromanageIt is a science fiction novel written by)William Gibson(It described a three-dimensional space of an infinite complex, created electronically, in which participants communicate with each other through computers, and then this representation permeated the imagination of the Internet pioneers who founded in 1990 the Cyber Frontier Foundation(EFF)Before the Internet became widely available to the public.[1]

Researchers and strategists differednIn naming the term cyberspace, they also differed in its definition; According to their different scientific specializations, and the purpose of employing this field in the service of the state, as American researchers tend to call it (cyberspace), while Russian researchers entrust it to call it (cyberspace) or (information space), which they believe is much broader than cyberspace. Thus, it gives a kind of protection to its users, while other researchers call it (cyberspace), and they believe that it is a system consisting of a set of elements, tools and procedures that can be added to the military system to enhance and modernize the military capabilities of the state. Thus, its geopolitical power is amplified.

The Cambridge English Dictionary defines cyberspace as: an electronic system that allows computer users around the world to communicate with each other or access information for any purpose.[2], as the Common Information Technology Dictionary defines cyberspace as: A system with a large Internet user base or even a well-designed interface.[3]The Russian-American summit defines cyberspace as: An electronic means through which information is created, sent, received, stored, processed and deleted.[4], as such defined asA global field within the information environment consisting of an interconnected network of information technology infrastructures, including the Internet, communication networks, computer systems, processors, and embedded controllers..[5]

2.2- Components of cyberspace:

Frederic Douzet, a professor at the French Institute of Geopolitics at the University of Paris, gave an accurate description of the components of cyberspace when he described it as: a structure consisting of accumulated and different layers that interact with each other in an organized manner, and he divided these layers as follows:.[6]

- Physical layer: It consists of a large group of equipment installed in an area and subject to deception; Given the geopolitical and natural requirements and their pressures in terms of building, destroying, connecting or separating them from the network from a strategic point of view that requires that.
- Logical Infrastructure Layer: It includes all services that facilitate the transfer of data between two points in the network, allowing the transmission of information divided into small packets of data from the sender to the recipient, and depends mainly on the establishment of a common language that makes it possible for all computers in the world to communicate with each other. Some are Internet Protocol (T/TCP These direct and choose the path through which data packets are transmitted between two networks, and the names that identify network elements or users, in addition to addressing that converts the series of numbers that represent addresses into words understandable to users.
- Applications layer: It consists of easy-to-use computer programs that allow everyone to use the Internet (web, cyber-mail, social networks, search engines, etc.) without knowing anything about computer programming, and the most prominent of these applications are those offered by a number of large companies such as: (Google, Facebook, amazon and others), to which users entrust their private data to be skillfully exploited by the marketing teams or intelligence services in the country. This data is stored on servers managed by private or public entities.
- Information layer: This layer consists of information and social interaction, and this section is sometimes called (cognitive or semantic), and includes users, competitions, and exchanges, which occur in real time across the world, and this layer is considered the most difficult in terms of understanding and representing it geographically , but its importance is great from a geopolitical perspective, for example: Once the most

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

active countries on (facebook), or determining the type of language in which content is available in certain regions of the world, or identifying revolutions on social networks, or disinformation campaigns against a government or institution, cyberspace consists of all these layers at the same time.

There are those who divide cyberspace into three components:.[7]

- The physical infrastructure of the business: It consists of a connected system, of computers, servers, networks and other network channels; Because initiating any action in cyberspace requires a computer connected to the network file so that it can move forward into the detailed depth of the virtual world.
- People: They are the ones who determine the nature of cyberspace and form its shape, from ideas and pieces of technology that can be found on the Internet and are the product of people's ideas, and there is no part of cyberspace unless it was initially created by people, as well as the cyber-attack is related to people, whether it is directed Against a state or a private company, people are both the perpetrators and the victims.
- Geographical: It constitutes the physical location of a particular element or user in the network. Although cyberspace does not have a physical presence in itself, devices and equipment have a physical location. Geography plays an important role in determining where people act, directing cyber-attacks, and with Who act, and the main factor in this dynamic is politics, geography and politics interact and determine the target of the cyber-attack.

3- Putin's strategy in Russian cyberspace:

Putin did not hide his determination to re-maximize Russian geopolitical power after years of deliberate humiliation by the United States and its allies in the North Atlantic Treaty Organization, NATO. His ambition to revive the legacy of the Soviet Union, which he repeatedly spoke of that its collapse was the disintegration of historical Russia.

President Vladimir Putin described NATO's expansion in Russia's periphery as a provocative unilateral seizure of land by the US-led alliance, which seeks to expand its geopolitical sphere of influence, and asserted that NATO by placing its military forces on Russia's borders violates the assurances given to Russia at the end of the Cold War He concluded that this unipolar and US-centric security model was unacceptable.[8],Although the United States is far from the theater of conflict in Europe, it leads NATO, which is expanding in the vicinity of Russia, and therefore Moscow finds itself facing additional security risks in Europe, represented by nuclear weapons in possession of France and the United Kingdom, as well as the United States of America deploying Semi-strategic nuclear weapons in Europe and NATO's conventional forces on Russia's borders, and this is what Moscow fears from a future threat to US nuclear weapons that are deployed today in its neighboring countries..[9],The Russian national security establishment, headed by Putin, believes that NATO's expansion in the vicinity of Russia was not only a land grab that upset the geopolitical balance in Europe, but also represented a violation of the assurances made by Western leaders to former Soviet President Mikhail Gorbachev at the time that in exchange for German reunification and NATO membership, no The alliance is expanding eastward.[10]

Putin has consolidated his control over Russia since his first term began in 2000, through a range of effective tactics ranging from controlling the media and social networking sites inside Russia to limiting the control of some major industries on the Russian economy, as well as restructuring some government institutions.

In 2000, President Vladimir Putin agreed to include the Internet within the doctrine of information security in the Russian Federation, and after the outbreak of the color revolutions in Georgia, Ukraine and Kyrgyzstan between 2003-2005, the wave of pro-democracy movements that used the Internet to spread information worried the Kremlin, which prompted Putin to intervene militarily in Georgia In 2008 to deter those conspiratorial revolutions of Western intervention via the Internet, as he described it.[11]

After 2012, Russian defense and security elites led by Putin recognized the importance of the internet and cyberspace in security threats, when the political opposition used them extensively to mobilize the public, first against elections to the Duma (Russia's lower house of parliament), and then against President Putin's re-election in 2011.[12]And after it became clear that the Internet and cyberspace are of great importance in the military field and the strengthening of offensive and defensive military capabilities, Russia used this strategic advantage to impose its control over the Crimea in 2014 and was able to achieve victory.

Therefore, since 2018, Putin's government has worked to further consolidate Russia's control over the Internet, and to strengthen Russia's defense capabilities in cyberspace by engineering the Internet

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

and directing Internet packets in a way that changes the shape of the Russian Internet for those inside the country, by submitting a draft law to Douma. The state isolates the Russian Internet, and the project came into effect on November 1, 2019, this operation was aimed at isolating, fortifying, and controlling the Russian Internet in order to reach the successful complete isolation of the Russian Internet .Ru Net in the future, to ensure that Russia does not have a security incident in cyberspace .[13]

Vladimir Putin constantly refers to sovereignty and strongly emphasizes that it is necessary to achieve Russia's national goals and prevent external threats, and therefore he finds that there is an urgent need today more than ever to accelerate the cyber-control measures of isolating the Russian Internet (Ru Net) About the global internet as long as there are direct and continuous threats to Russia's security. The major countries today view cyberspace as an effective means to defend their sovereignty, stop cyber-attacks on its infrastructure, and ensure its national security and national defence. There is also great concern about the protection of vital infrastructure, which if disrupted or Sabotage can cause great damage to the civilian population, as experts believe that the risks of cyber-attacks may cause the deaths of millions of civilians or even bring down entire countries.

It seems that Putin's government was aiming to isolate the Russian Internet from the global Internet, to fortify Russia from the inside, and to practice its cyber activities from outside its geographical borders, in order to target adversary countries and banish suspicions directed at Russia as a confirmed actor of disruptive cyber-attacks.

Russia, especially the regime of President Putin, views the information confrontation as a continuous zero-sum geopolitical competition between great powers, political and economic systems and civilizations. Therefore, it views the information space from a very geopolitical perspective, and believes that its local information space represents a continuation of the borders of the regional state, which it sees as It is constantly violated by foreign interventions, in the belief that the security of Russia can be best ensured only by exercising control over its borders and in its perceived border area.[14].

Russia's approach today in cyberspace under Putin's leadership is unique, as Russia is constantly adapting to new conditions and technology, which has made it a difficult figure in the geopolitical confrontation.

This strategy and this shift in Russia's foreign policy was announced by Russian President Vladimir Putin in his press conference in December 2018 when he said: The global influence of the United States is over, and he reproached the United States about having a sense of impunity, saying that this is the result of the monopoly of a unipolar world, Fortunately, he added, this monopoly is fading away, and it is about to end, and that this provides an opportunity for Russia to fill the void left by the United States and become once again a great power with a decisive voice in the international community.[15]

The apparent shift in Russian foreign policy and Russia's return as an important global player is only a result of the Kremlin's behavior developed during the era of President Vladimir Putin and its continuous demand for a distinct area around Russia's immediate periphery, and its refusal to accept the security system after the Cold War in Europe, which is what MHis decisive assertion in launching the war on Georgia in 2008, the annexation of Crimea in 2014, and the Kremlin's recent expansion of the geographical scope of its foreign policy through active presence in parts of the world, especially the Russian project in Africa, Latin America, the Middle East and other regions Another, which Russia is completing today in its geographical vicinity through its invasion of Ukraine on February 24, 2022.

Recently, Russian foreign policy has reflected the Kremlin's desire to take advantage of the favorable external environment and get rid of the unipolar international system led by the United States of America. Since Putin's return to the presidency in 2012, his record has been strengthened by what the Russian authorities consider several important victories, including: his refusal to recognize The legitimacy of the Kyiv government after the overthrow of the government of the pro-Russian former Ukrainian President Viktor Yanukovych, and requested the approval of the Russian Parliament to send military forces to Ukraine to protect Russian interests. joining Russia.[16],Then he continued the war in eastern Ukraine and recognized the popular republics of Donetsk and Lugansk, along with the military deployment in Syria, the tense military confrontation with the West in the Baltic and Black Seas, and interference in the internal politics of the United States and Europe, these issues re-emerged Russia as a superpower with great capabilities to project power. And a strong player on the international scene, and cemented Putin's reputation as a strong leader and a skilled politician. These victories also demonstrated to

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

the world Russia's tendency to face great risks above its weight, along with its improved capabilities in the areas of multiple forces, land, air, sea, cyber and information operations, and this expansion project of the new Russia. Which is led by President Vladimir Putin is no longer implied, but has become clear today after the recent Russian invasion of Ukraine.

4- Russian cyber operations abroad:

It is believed that the service (FSB: federalnya sluzhba bezopastnosti) is Russia's main service for coordinating cyber propaganda and disinformation campaigns, and is responsible for the maintenance and operation ofSORMThe country's internal cyber surveillance system**,** has This service came as a successor to the Federal Agency for Government Information and Communications (FAPSI) that was active in the nineties**.**

In 2003 it was dissolved)FAPSI) and absorb its components in (FSB) And (MVD(Federal Protection Service of the Russian Federation, and)FSO RS) And(SVR), which is the Russian Foreign Intelligence Service responsible for coordinating most of the country's internal and external cyber operations, and this service has maintained the highest levels of command for cyber operations outside Russian borders, It controls the supervision of the field of communications, information technology and mass communications, which is responsible for supervising the media affiliated with the Ministry of Interior and organizing its work that focuses on cybercrime.[17], after The dissolution of the Soviet Union, the intelligence responsibilities of the (KGB)To newly established branches of intelligence, including the Federal Security Service(FSB),and foreign intelligence service (SVR),The Main Directorate of the General Staff of the Armed Forces of the Russian Federation(GU),known BMain Intelligence Directorate(GRU) during the Soviet era.

These three groups play major roles in the Russian cyberspace, and it is believed that(FSB)Principally responsible for Russian hacking, media reports and federal indictments indicate that it has significantly developed its cyber capabilities by relying on the selection and recruitment of talented individuals into the Russian cyberspace..[18] , Today it is responsible for counterintelligence, surveillance and oversight in the Russian Federation and has become heavily involved in external cyber operations, and for the expansion of Russian geopolitical power and influence in Europe.

as it works (SVR) to carry out a wide range of intelligence activities, primarily focused on the collection of foreign intelligence, It mostly conducts human intelligence operations, and its cyber capabilities are not comparable to those of the other two groups; This is because the work of the Russian Military Intelligence is different from other intelligence services, as it is an intelligence service of the Russian Armed Forces. GRU It is described as the most active group in the Russian cyberspace, and has access to large amounts of resources to support its cyber operations, and it is believed that (GRU)is the parent organization ofAPT28) and team (Sandworm), while preparing (APTs) including (Turla) And (APT29) And (Palmetto Fusion) And (Gamaredon Group) affiliated with the service(SVR).[19]

In view of the large number of organizations or sub-networks affiliated with the major groups above, they have been divided into the following:

- **Group(AP28)/** Dubbed Fancy Bear, and it is believed that they belong to(GRU),This group started its activities since 2004, and it is the most famous group (PT) Russian and the most influential; Because of her success in penetrating the US Pentagon in 2015, then she succeeded in hacking the networks of the Democratic National Committee in 2016, as well as her interference in the 2016 US elections, and in 2018 she was accused of hacking the US World Anti-Doping Agency, and US nuclear facilities.[20]It is also accused of targeting US research institutes affiliated with the Corona virus in 2020.
- **Group (AP29)/** They are called Cozy Bear, and it is believed that they belong to(SVR And FSB),This group has started its activities since 2008, and is considered one of the most PT The Russian news agency reported that it had succeeded in penetrating the US Treasury and the Internet and Communications Policy Agency, as well as the unclassified networks of the White House, the State Department and the Joint Chiefs of Staff in the United States of America, and succeeded in stealing information from these sites. .[21]
- **(APT Turla)/** This group has started its activities since 2004, and represents a highly sophisticated cyber threat. It has targeted more than 45 countries, focusing on government industries, embassies, the army, education, research and pharmaceutical companies.[22], no less important Turla about the importance of (AP28) And (AP29) In terms of its success in carrying out cyber operations, it has targets

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

of a global geographic scope, despite its focus on Western Europe and East Asia.[23]

• (**Sandworm Team**)/ This team has been active since 2009, and is believed to be associated with(GRU The hackers of this team are distinguished by their high ability to hide and defend their presence with infiltrated systems for a long time, and the goals of this team differ from those of its counterpart(AP28), they are related to energy, as the team uses (Sandworm malicious program known as Black Energy) They are constantly updating it to target energy-related infrastructure, and in 2015 it targeted a Polish energy company, as well as carried out destructive electronic operations in Ukraine during 2015 and 2016 targeting and shutting down the Ukrainian electricity network.[24]

• (**Saw Palmetto Fusion**)/ This team has been active since 2015, Described It is relatively new and is believed to belong to (FSB), this team focuses on targeting energy infrastructure similar to the work of the team(Sandworm Team) The aforementioned, but it focuses its objectives on the countries of Ireland, the United Kingdom, Turkey and the United States of America .[25]

• **(Gamaredon Group)/** This team has been active since 2013, described as a Russian cyber espionage team, and is believed to be linked to the Federal Security Service(FSB),It is directed to target military organizations, NGOs, the judiciary, and non-profit organizations in Ukraine[26].

• **(Energy Seekers: Dragonfly & Dragonfly2.0)/** They are two types of access point transmitters and receivers that focus primarily on energy-related targets, and this group is so similar that there is disagreement among cyber security analysts about whether they are actually one group or two separate groups from each other, but in the latter presented Cyber security experts have factual evidence that they are two separate groups, and they have been active (Dragonfly) since 2010, and it has been targeting countries around the world, but it focuses its attacks on Europe and the United States of America, and after several cyber security companies issued in 2014 reports on the activity of (Dragonfly(The group suddenly disappeared, but)Dragonfly2.0It was active in late 2015, and launched a campaign targeting the western energy sector. This campaign set its goals in the countries of the United States of America, Switzerland and Turkey[27].

It should be noted that there are very many other electronic hacking groups and networks that are linked to the Russian government, but we did not address them because they are less high and less influential in the electronic attacks they have carried out against countries that Russia believes are an explicit threat to Russian sovereignty.

5- Cyberspace and its impact on the growing geopolitical power of Russia:

Russia resorted to using cyber weapons after it felt the increasing danger represented by the emergence of a new geopolitical division of Europe. This matter brought about a major shift in the Russian strategy with regard to European security, especially after the United States, led by NATO, began deploying its weapons in Russia's vicinity, and supporting a united Europe with the aim of Expand its capabilities, but Russia did not stand idly by in the face of the interventions of NATO and the West in its vicinity.

In 2008, the Russian military forces moved to invade Georgia and were able to achieve victory in the war, but this war sent two very distinct messages, the first containing a strongly worded warning to the West to stay away from the circle of Russia's distinct interests, while the second message to Russia revealed the country's need for a capacity that exceeds its nuclear arsenal to defend its interests and deter anyone who infringes upon it, especially after Russia shocked the United States and NATO with its cyber capabilities that it used in support of military operations and managed to seize Crimea in March 2014.[28]

Russia has for many years relied on its nuclear weapon as a guarantor of peace and security among the great powers and constantly stresses its importance to Russia's position as a great power and a source of continued power and influence in light of the development of the geostrategic race, and it is a necessity to deter Washington from any possible attack on Russia or any coercive threats against it, but Although Russia's nuclear weapons were indispensable as a safeguard against Western interference in Russia, they were less useful when it came to intervening in external crises and projecting Moscow's interests beyond borders. The nuclear arsenal was of little use when it came to deterring NATO's circular expansion It was ever closer to Russia's borders and securing a geopolitical sphere of influence around its periphery, a long-overdue Russian goal.

Therefore, Russia today looks at cyberspace as a weapon much more powerful than nuclear weapons and more influential in modern cyber war to defend its sovereignty and enhance its position as a great power, in addition to deterring Western threats against

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

Moscow and stopping NATO's expansion in its regional surroundings represented by the former Soviet Union countries in light of There is a clear inability on the part of states to provide official evidence identifying the perpetrator of cyber operations to be legally convicted before international courts.

Therefore, cyber weapon has become a critical component of warfare; Because of the increasing geopolitical threats and conflicts and their intertwining in today's world, and achieving information supremacy in cyberspace has become Russia's primary goal, and the structure of the state, and that mixed operations today are strongly based on cyber operations, and they are simply a continuation of those Russian measures, Although the Russian Ministry of Defense has been slow to embrace the Internet and information space; For structural and ideological reasons, the Kremlin has worked to enhance cyber-attack and give the offensive cyber a greater role in traditional Russian military operations, as well as enhancing the defensive cyber capabilities of the Russian armed forces.[29]

Russia's cyber activities are on the riseaims to advance Moscow's broader geopolitical aspirations, as well as affirm Russia's relentless claims to great-power status; In order to strengthen its geopolitical hegemony over its declared sphere of influence; to destabilize the West and distract it to the point where it is unable to effectively confront Russian actions on the other hand; As well as to undermine the role of hostile governments and Western power structures that have become close to their geographical surroundings such as NATO and the European Union, and therefore it is likely that Russia today uses all available means to achieve its goals of maximizing its geopolitical power in its regional surroundings, and expanding its geostrategic influence outside its borders, especially after the cyber field has become one of the main theaters of Russian military and political operations.

What is new in Russia's approach today is the increasing reliance on new tools and methods, especially in the cyber field, to achieve a strategic advantage that allows Moscow to excel in some geopolitical conflicts. The information space opens up vast and unequal possibilities that reduce the enemy's combat ability.[30]

Because it allows the dissemination of propaganda and misinformation, including distortion of facts and the increase of fabricated information in order to manipulate the feelings of public opinion, and makes Russia more ready to strike the enemy in multiple ways simultaneously using diplomatic, information, military and economic tools of national power and to achieve Russia's geostrategic goals and ambitions.

These ambitions were confirmed by President Vladimir Putin when he spoke about the close link between technology, innovation and cyberspace and their relationship to national security and international power .At the time, he said: (The country that leads artificial intelligence will be the ruler of the world), and this statement may be somewhat exaggerated, but it is not excluded at a time when the ability to innovate has become an effective source of national strength and national security, and strength has become different requirements shaped by technological changes and cyberspace.[31]

Russian military experts have also consistently emphasized since the early 2000s that Russian deterrence strategies should use non-military measures such as information technology, which contribute to the engagement of the target country's public institutions, including the media, cultural and religious institutions, religious non-governmental organizations, and political movements. foreign, and employing and maintaining these mixed tactics and then using them in cyber war, and military capabilities are used only in the event that non-military methods are unable to achieve their goals.

And because the security environment along Russia's periphery is unstable, it constitutes an internal challenge facing Moscow today more strongly than ever, which has led to a state of instability and the escalation of local conflicts in this region. This belief was issued by the national security establishment and the Russian political elites, Described as the result of a push by the West from the countries of the former Soviet Union to compete with or openly hostile to Russia in every strategic direction. [32]Therefore, Russia recently resorted to intimidating its geographical neighbors and deterring them from antagonizing Moscow, either by threatening with nuclear weapons or by using cyber weapons through information warfare and cyber-attacks. This cyber feature that Russia added to its military capabilities was not available in the past. Rather, it was relying heavily on nuclear weapons in deterrence operations and ensuring the sovereignty of the state, but Moscow was able to successfully develop its cyber capabilities and combine them with military capabilities and test them in the invasion of the Crimea, becoming Russia Today, it is one of the most powerful countries in the world in the field of cyberspace .

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

Over the past two decades, the Russian military and political leadership underwent a fundamental modification to its concept of war and the role of electronic operations in this advanced view, which brought about a major shift in Russia's perceptions of war, from a general consensus that the basis of war is armed violence and non-military measures to that capabilities are Cyber and strategies that support modern Russian military cyber-attacks and information operations are one of the most important areas of warfare .[33]

The experiences of Georgia and Ukraine have profound effects not only on those two countries, but also on the countries of Armenia, Azerbaijan, Belarus, Moldova, Poland and other countries that fall within Russia's objectives. Its geopolitical field and its political neutrality, at the very least, these countries lack the security protection that they have always been promised by the West and NATO, and this is what makes them constitute an open battlefield between the West and Russia in light of the West's and NATO's assurances that they are not ready to abandon these countries to the Russian sphere. .[34]

The conflict in Ukraine provided great opportunities for Moscow to improve its cyber-information technologies and shady information. Today, Russia is seen as a world leader in the cyber field, even if it is difficult to accurately determine its cyber capabilities. There are professional players in this field who have implemented several prominent cyber-attacks. Attributable directly to groups linked to the Russian government, for example the Russian government is suspected of supporting and sponsoring cyber-attacks on energy infrastructure around the world, particularly in Ukraine and the Baltic states.

There is also an explicit recognition by policy makers in the European Union that cyber operations attributed to Russia have contributed significantly to amplifying the Russian geopolitical power in Europe and increasing its influence in at least 27 countries of Europe and North America since 2004, and there is a report submitted by the Intelligence Agency The Estonian Foreign Ministry in 2018, stressed that cyber threats to the West are increasing and that most malicious cyber operations are due to Russian cyber activity, and New Zealand, Australia and many European Union countries are attributed to Russia as being responsible for malware attacks (wannacry And Not petyaexperienced by these countries.[35], In 2008, researchers presented clear evidence that Russia used computer networks in its cyber operation during its invasion of Georgia, and described those operations as having played an active role in Russia's military progress.[36]There are also accusations of Moscow carrying out destructive cyber-attacks on the Ukrainian electricity network and infrastructure during 2015 and 2016, as well as hacking the US Pentagon in 2015, targeting the US presidential elections in 2016, as well as targeting the French presidential campaign of President Emmanuel Macron during 2017 and 2018 .

It is also believed that in June 2017, the Russian military launched an attack Not Petya Cyber-attack against Ukrainian networks, this program quickly spread around the world, causing billions of dollars in damage across Europe, Asia and the Americas, and is part of a Russian effort to destabilize Ukraine.[37]These accusations were strongly rejected by Russian President Vladimir Putin, describing them as nonsense, as Russia not only denies its responsibility for these activities, but also claims that European countries were interfering in its presidential elections and that a new era of information war against Russia is about to occur.[38]

The great development of Russia's strategic thinking and its escalating cyber approach towards the countries of its geographical surroundings and other places of the world, and the development of its vision of modern war, does not take place in a strategic vacuum, but rather is empowered and shaped through broader political considerations. Cyber operations are unlikely to be unmotivated, Rather, it is part of Moscow's evolving approach to unequal competition with these countries To achieve certain ends that are a reflection of its broader strategic objectives This matter clearly contributed to the inflating of Russia's geopolitical power. What are the military moves towards the Crimea and its occupation in 2014, the military presence in Syria and the movements of Russian military ships in the Mediterranean Sea, but an actual shock to the institutions of national security and foreign policy in Europe and the United States of America, which This is confirmed by the last Russian occupation of Ukraine in 2022, which shocked the entire world and imposed a new geopolitical reality in Europe.

In the future, the Russian government is likely to continue its cyber-attacks and amplify its geopolitical power abroad; Because it realizes that it can do so as long as there is great difficulty in presenting real evidence that officially condemns it, and as long as there is a possibility of relative impunity, and this is something that has increased Russia's geopolitical power in the countries of Europe and the West.[39]Russia views the information space from a

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

very geopolitical perspective, and is keen to preserve its local information space, because it represents a continuation of the territorial state borders, which Russian defense experts see as being constantly violated by the interventions carried out by the West.

Moscow also considers the conflict in the information field to be continuous and never ending, and therefore it believes that its national security is threatened in the field of information by countries that are trying to dominate this field while developing its concept of information warfare, and on this basis the Russian Ministry of Foreign Affairs provided a comprehensive understanding of the concept of information warfare. Cyber security By focusing on threats related to the technical and psychological aspects of information warfare, Russia's military doctrine since 2010 has raised the status of information warfare, and emphasized the increasing reliance on information warfare in contemporary military conflicts.[40]

Russia's recent military moves or even cyber operations, specifically in its geographical surroundings, have increased its geopolitical influence and contributed to the amplification of its power to re-emerge as a strong player on the international scene. Because it blocked the way to a more serious geopolitical imbalance in the European continent resulting from the unprecedented expansion of NATO and the European Union in Central and Eastern Europe, which makes Russia in a position of weakness, and this is what Moscow does not accept according to the opinions of Russian strategists, and given the absence of major changes in the Russia's view of NATO's movements with the support of the United States, and the view of the latter two on Russia, the adversarial relationship will remain a major feature of the Euro-Atlantic system in the foreseeable future, especially after the recent Russian occupation of Ukraine, which complicated the matter a lot. Therefore, it requires a political and not a military solution to end this confrontation.

The development of Russian capabilities in cyberspace and Moscow's willingness to use cyber weapons at any time, amplified its geopolitical power and made it an additional threat to the general national security of the United States of America in particular, and to the cyber infrastructure of the world in general in the absence of recognized territorial borders in the world of the Internet.[41]

For example, in 2008, Russia combined its cyber capabilities and military operations to increase its strategic advantage, and this enabled it to penetrate Georgia's cyber network and enhance the progress of its army in the war against weak Georgia. .[42]

Russia's development of its cyber capabilities has given it the opportunity to carry out espionage and data theft from adversary countries across wide geographical areas. Strategic planning at present is matched by the political desire to harm the adversary countries and the determination of the geographical locations of the targeted countries. Here lies the danger of cyberspace in the geopolitical perspective.

CONCLUSIONS:

1- that Geopolitics is an essential and indispensable tool for understanding and analyzing new cyber challenges; As long as there are close links between cyberspace and geography, cyber threats do not occur separately from a physical place, but rather stem from a physical infrastructure for work and a geographically defined area that provides a basis for countries to deal with them in creating their strategies in cyberspace, and the main factor in this dynamic is politics, and geopolitics It is the one that interacts and determines the goal of the cyber-attack, and here geopolitics is firmly concentrated in the cyber space.

2- Russia today views cyberspace as a weapon much more powerful than nuclear weapons and more effective in modern cyber warfare; To defend its sovereignty and enhance its position as a great power, in addition to deterring Western threats against Moscow and stopping the expansion of NATO in its regional environment represented by the countries of the former Soviet Union.

3- Cyber weapon has become a critical component of warfare; Because of the increasing and intertwined geopolitical threats and conflicts in today's world, and achieving superiority in cyberspace has become Russia's primary goal, and the structure of the state, and that the mixed Russian operations today are strongly based on cyber operations.

4- President Vladimir Putin is trying to isolate the Russian Internet from the global Internet in the future, and create an Internet network for Russia; This is in order to fortify Russia from within and to practice its cyber activities from outside its geographical borders to target adversary countries and remove suspicions directed at Russia as a sure actor of sabotage cyber-attacks.

5- Russia's military movements or even its cyber operations in recent times, specifically in its geographical surroundings, are part of the fundamental shift in Russian foreign policy. This has increased its geopolitical influence and contributed to

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

the amplification of its power to re-emerge as a strong player on the international scene. Because it blocked the way to a more serious geopolitical imbalance in the European continent resulting from the unprecedented expansion of NATO and the European Union in Central and Eastern Europe.

6- The Russian cyber capabilities are highly advanced, and Moscow has demonstrated its use of these capabilities alongside its military capabilities in the war on Georgia and Ukraine, as well as its willingness to use its offensive cyber capabilities in situations other than war; To influence the political, economic and social outcomes in its neighboring countries at odds with it.

7- Russia has benefited greatly from cyber experts in identifying vital locations and bank targets for the targeted countries; To facilitate the task of the movement of military units in the war on the ground, and to provide the Air Force with a bank of opponent targets and their destruction, as well as to determine safe locations within the borders of the target country; To facilitate the task of the movement of military units in moving and positioning in safe locations far from the strikes of hostile countries that want to target them.

8- The rivalry between Russia and the US-led NATO is likely to remain a major feature of the Euro-Atlantic system for the foreseeable future; This is due to the absence of major changes in Russia's view of NATO's movements, and the latter's view of Russia, in addition to the recent Russian occupation of Ukraine, which has complicated the matter a lot, which calls for a political, not a military, solution to end this confrontation.

9- In the future, the Russian government is likely to continue its cyber-attacks and amplify its geopolitical power abroad, especially attacks targeting American interests in the countries of the former Soviet Union. Because it realizes that it can do so as long as there is great difficulty in presenting real evidence that officially condemns it, and as long as there is a possibility of relative impunity, and this is something that has increased Russia's geopolitical power in the countries of Europe and the West.

REFERENCES:

Frédérick Douzet, Understanding Cyberspace with Geopolitics In Hérodotem, Volume152-153, Issue1-2,2014, pages3to21, International Edition Cairn, PDF, P6, Available online at:https://2u.pw/AVZVA

American Dictionary, Cyberspace, Available online at:https://2u.pw/j56iX Technology Dictionary, What Does Cyberspace Mean?, Available online at: https://2u.pw/Qj9qD

V Kh Fedorov et al, Cyberspace: Key Properties and Traits, Journal of Physics:Conference Series,2021J. Phys.: Conf. Ser.2096012039, PDF, PDF2,Available online at:https://2u.pw/4NzNx

Uche Mbanaso, Eman Dandaura, The Cyberspace: Redefining A New World, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN:2278-8727, volume17, Issue3, Ver. VI (May - Jun.2015), PP17-24, PDF, P18. Available online at: https://2u.pw/viygj

Frédérick Douzet, Understanding Cyberspace with Geopolitics, Op.Cit, P4.

Emily B. Bordelon, Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law, A Senior Thesis submitted in partial fulfillment of therequirements for graduation in the Honors Program Liberty University Fall,2016P6,7.

Eugene Rumer, Russia and the security of Europe, Carnegie Endowment for International Peace Publications Department, Washington,2016, P10.

Wolfgang Richter, NATO-Russia Tennis: Putin Orders Invasion of Ukraine, Available online at:https://2u.pw/lpALr

Eugene Rumer, Russia and the security of Europe, Op.Cit, P10.

Justin Sherman, Reassessing RuNet Russian Internet Isolation and Implications for Russian Cyber Behavior, Scowcroft Center for Strategy and Security,2021, P3.

Janne Hakala, Jazlyn Melnychuk, Russia's Strategy in Cyberspace, Published by the Nato Strategic Communications Center of Excellence, Latvia,2021,P12 .

Justin Sherman, Reassessing RuNet Russian Internet Isolation and Implications for Russian Cyber Behavior, Op.Cit, P2,3.

Janne Hakala, Jazlyn Melnychuk, Russia's Strategy in Cyberspace, Op.Cit, P5-9.

Robert E. Berls Jr., Strengthening Russia's Influence in International Affairs, Part I: The Quest for Great Power Status, Jul13,2021, Mean?, Available online at:https://2u.pw/j4PZv

Encyclopædia Britannica, Vladimir Putin president of Russia, Available online at:https://2u.pw/zv8PB

Michael Connell, Sarah Vogler, Russia's Approach to Cyber Warfare, Op.Cit, P6.

Andrew S. Bowen, Russian Military Intelligence: Background and Issues for Congress, Congressional Research Service, PDF, November24,2020,P16 .

Mikk Marran, International Security and Estonia, Estonian Foreign Intelligence Service, PDF,2018,P55-57.

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 10, May,2022
ISSN: 2749-361X

MITER ATT, CK Corporation, Group AP28, Available online at: https://2u.pw/LGpRB
Arab21, Hackers infiltrate the US Treasury... and sources talk about their identity, Available online at:https://2u.pw/GoZT9
MITER ATT, CK Corporation, Group AP28, Available online at: https://2u.pw/yOtlN
Conor Cunningham, Russian Federation Information Warfare Guide, November 12,2020,Available online at:https://2u.pw/wVqHp
MITER ATT, CK Corporation, Group AP28, Available online at: https://2u.pw/Dy5IT
WIRED, by ANDY GREENBERG, Your Guide to Russia's Infrastructure Hacking Teams, Which of Russia's hacking groups is targeting American energy utilities?, JUL12,2017, Available online at:https://2u.pw/wJq49
MITER ATT, CK Corporation, Group AP28, Available online at: https://2u.pw/0w6ES
Conor Cunningham, Russian Federation Information Warfare Guide, November12,2020,Available online at: https://2u.pw/gAtVP
Eugene Rumer, Russia and the security of Europe, Op.Cit, P11.
Jarno Limnell, Russian cyber activities in the EU, European Union Institute for Security Studies (EUISS)chapter6,PDF,2018, P66,67.
Andrew J. Duncan, New 'Hybrid War' or Old 'Dirty Tricks'? The Gerasimov Debate and Russia's Response to the Contemporary Operating Environment, Canadian Military Journal, Vol.17, No.3,PDF, Summer2017, P8
James A. Lewis, Technological Competition and China, Center for Strategic International Studies, November2018, P1.
Eugene Rumer, Russia and the security of Europe, Op.Cit, P1.
Bilyana Lilly, Joe Cheravitch, The Past, Present, and Future of Russia's Cyber Strategy and Forces, Op.Cit, P131,132.
Eugene Rumer, Russia and the security of Europe, Op.Cit, P2.
Jarno Limnell, Russian cyber activities in the EU, Op.Cit, P68.
Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald,Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, Report World War C : All rights reserved of FireEye, Milpitas, CA, PDF,2014,P12.
Analytic Exchange Program, commodification of cyber capabilities A grand cyber Arms bazaar, Public - private,2019, PDF, P13.https://2u.pw/ThCz0
Jarno Limnell, Russian cyber activities in the EU, Op.Cit, P71.
Bilyana Lilly, Joe Cheravitch, The Past, Present, and Future of Russia's Cyber Strategy and Forces, Op.Cit, P130 .
Jarno Limnell, Russian cyber activities in the EU, Op.Cit, P70.
Bilyana Lilly, Joe Cheravitch, The Past, Present, and Future of Russia's Cyber Strategy and Forces, Op.Cit, P134 .
Yancey, Cyril K, "Cyber Security: China and Russia's Erosion of21st Century United States' Hegemony," McNair Scholars Research Journal: Vol.12, Article9,2019, P113.
Emily B. Bordelon, Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law, Op.Cit, , P7.