ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 03 No. 02. April-June 2025.Page#.1287-1302
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Russia's Digital Diplomacy and Cyber Governance: Strategic Narratives, Hybrid Tactics, and Global Implications (2000 2025)

Sami ul Haq
PhD Scholar International Relations
Karachi University
samiulhaq122@icloud.com

Abstract
This paper explores the evolution and strategic function of Russia's digital diplomacy from the early 2000s through 2025, examining its role in shaping international cyber security norms. Drawing on theories of realism, liberalism, and constructivism, the study situates Russia as both a cyber power and a diplomatic actor actively contesting Western-led frameworks. Initially characterized by broad, unfocused public diplomacy efforts, Russia's digital outreach matured into a sophisticated fusion of strategic communication, public diplomacy, and state-backed disinformation. From targeting marginalized groups via social media to lobbying for cyber sovereignty at the United Nations, Russia has transformed from a reactive to a proactive force in global cyber governance. The paper investigates how digital diplomacy evolved into an offensive instrument of influence, combining overt messaging with covert campaigns aimed at reshaping narratives and undermining liberal institutions. Case studies from 2013 to 2025 including bilateral treaties, BRICS cyber partnerships, and influence operations around U.S. elections highlight this shift. The research concludes that Russia's cyber diplomacy has not only redefined the tools of statecraft but also accelerated the splintering of cyberspace governance into competing global visions.

Keywords: digital diplomacy, Russia, Cyber Empire, soft power.

Introduction

Defining International Cyber Security.

International cyber security refers to the collective strategies, policies, and cooperative efforts by states and international bodies to safeguard the global digital domain from cyber threats that transcend national borders (Sustainability Directory, 2025). In an era where critical infrastructure, economic systems, and communications are interlinked worldwide, a single cyberattack can cascade across countries, endangering international stability. Recent years have seen a sharp rise in state-sponsored cyberattacks and incursions often targeting critical infrastructure and democratic institutions underscoring that no nation is immune and no nation can address these threats in isolation (Council on Foreign Relations,). The significance of international cyber security, therefore, lies in its role as a *global public good*: ensuring a secure and stable cyberspace for all nations is essential for protecting not only national security but also the health of the global economy and the integrity of international peace (Sustainability Directory, 2025). This has elevated cyber security to a high-priority issue on the international agenda, demanding collaborative solutions and mutual defense arrangements among states (Council on Foreign Relations,).

Diplomacy's Role in Cyberspace.

Diplomacy traditionally defined as the art of managing international relations through negotiation has increasingly extended into the cyber realm as states recognize that technical measures alone cannot solve transnational cyber challenges. *Cyber diplomacy* is broadly defined as the use of diplomatic tools, dialogue, and international negotiations to address issues arising in and through cyberspace (American Foreign Service Association). Those issues span security topics (like cyber defense, cyber warfare, and espionage), economic concerns (such as intellectual property theft and digital trade), and human rights questions (such as internet freedom and privacy) (American Foreign Service Association,). In practice, cyber diplomacy involves engaging allies and adversaries alike to develop common norms, share threat information, and build frameworks for conflict prevention in the digital domain. Diplomatic engagement is crucial for building trust and transparency, which help reduce the risk of misperceptions or escalations during cyber incidents. Indeed, experts emphasize an urgent need for cooperation among states to mitigate threats like cyberattacks on critical infrastructure, electronic espionage, and other offensive cyber operations that could destabilize international security (Council on Foreign Relations,). By leveraging diplomacy, states seek to establish rules of the road for cyberspace for example, agreeing not to attack each other's critical services in peacetime and to create communication channels for managing cyber crises. Through multilateral forums and bilateral dialogues, diplomacy provides a platform for nations to reconcile differing perspectives on cyber governance and to coordinate responses to cyber threats before they spiral into broader conflicts (Zinovieva, 2023). In short, diplomacy serves as a *bridge* in cyberspace, allowing nations to collaboratively address a domain that is borderless and often rife with ambiguity.

Russia as a Significant Case Study.

Russia provides a particularly educative case study in international cyber security diplomacy due to its dual role as an active shaper of a major cyber power and cyber regime criteria. Along with the United States and China, Russia is widely considered one of the world's major cyber powers, which has a significant impact on sophisticated cyber abilities and global cyber threats. This situation means whether Russia's action in cyberspace results in international security from aggressive operations or diplomatic initiatives. At the same time, Russia has been at the forefront of cyber diplomacy efforts for more than two decades, often advocating a vision of cyberspace regime that challenges Western liberal attitudes. Ever since it raised the issue in the United Nations in 1998, Moscow has pushed for a new international rule to regulate state behavior in the information space. It continuously emphasizes "international information protection" (a concept that argues for sovereign state control over cyber threats) and for sovereign state control over cyberspace, reflecting Russia's concern that liberal "rule-based international orders" in cyberspace do not adequately protect their interests.. Russia's cyber diplomatic posture rooted in its national experience and strategic culture has thus involved contesting many of the norms championed by Western states and proposing alternative principles. For example, Russian diplomats have persistently called for a binding international treaty on cyberspace, greater state sovereignty online, and restrictions on what they term "information warfare" (such as the spread of destabilizing content). These positions make Russia a pivotal actor: it can be seen as a norm entrepreneur offering a competing narrative of cyber governance, as well as a potential spoiler when consensus leans toward Western proposition (Kurowska, 2019). Studying Russia's role is therefore crucial to understanding how diplomacy can promote international cyber security, since

Russia has both significantly influenced the development of global cyber norms and, at times, tested the limits of those very norms through its cyber activities. This case also illuminates the broader geopolitical dynamic in cyber negotiations between cooperation and competition, sovereignty and openness in today's multipolar world. In the following sections, we outline the theoretical lenses for examining cyber diplomacy, and then delve into Russia's historical engagement in cyber diplomacy from the early 2000s to the present, highlighting how diplomatic initiatives and strategies have evolved in tandem with the shifting cyber threat landscape.

Russian Digital Diplomacy: A Rising Cyber Soft-Power?

Russian digital diplomacy embodies a state-directed communication strategy that utilizes social media and internet platforms to interact with global audiences. The formal launch is sometimes attributed to 2012, when Russia's Ministry of Foreign Affairs commenced a state-sponsored initiative to disseminate political narratives through social networks, particularly by establishing its inaugural official YouTube channel. Nonetheless, the foundation for Russian digital diplomacy had already been established through prior iterations of "twiplomacy" the calculated employment of Twitter by state-affiliated organizations such as RT (Russia Today), RIA Novosti, and the Voice of Russia, in addition to the personal accounts of Russian officials engaged on international platforms. Unlike countries such as the United States, France, Germany, Iran, and China who rapidly emerged as global leaders in digital public diplomacy and adeptly influenced public opinion Russia's initial online diplomatic initiatives were limited and lacked strategic coherence until approximately 2013 (Simons, 2015). In later years, Russia reestablished its presence in the digital domain by revitalizing Cold War-era propaganda methods in a modern context. This paper examines contemporary tactics utilized by Russian digital diplomacy, which integrate provocative, exploitative, and strategic rhetoric with proactive information distribution. This analysis focuses on public diplomacy and interconnected topics of digital diplomacy, which relate to widespread perceptions such as publicity and strategic communication. Public diplomacy typically includes initiatives funded by the government spreading education, culture, religion, sports, and internet platforms across many fields to carry forward national security objectives and foreign policy strategies.

Digital diplomacy, or internet diplomacy, is an essential subgroup of public diplomacy, mainly related to promoting national political purposes in cyberspace. Digital diplomacy, often confused with propaganda or strategic communication, involves both clear and vested efforts to reach foreign audiences through online information campaigns. Many major states currently use a mixture of public diplomacy, internet engagement, and strategic communication to influence political mobility in foreign countries. These operations may include electoral arbitration, governance instability, creative diplomacy, and international cooperation. Russia's employment of both soft and harsh power in its digital diplomacy indicates a remarkable change in the effect of global dynamics (NYE, 2018).

An important catalyst for this change is the emergence of social media, which has introduced an unexpected new aspect to public diplomacy. The immediacy and emotional quality of digital contacts facilitate swift mobilization occasionally within hours. The political landscape in reality increasingly reflects tendencies established online. Events include the Arab Spring (2010–2011), the Russian protests of 2011, the Ukrainian Euromaidan of 2014, and the demonstrations in Iran in 2017 have all been shaped by social media discourse. Digital platforms offer methods such as targeted advertising, algorithmic content amplification via likes and shares, and segmentation

based on political interests, enabling strategic actors to exert influence at a little cost. Engagement from devoted followers amplifies messages within public awareness, particularly on platforms such as Facebook and Twitter. The expansion of Internet availability has enhanced digital diplomacy. In the United States, more than 87% of the population utilizes the Internet, ranking it 13th worldwide in digital accessibility. Russia ranks 40th with a percentage of 70.5% (The Global Information Technology Report 2016: 163, 189, 239). As an increasing number of users rely on social media for news and political discourse, the impact of these platforms escalates. The consumption of political content has transitioned from traditional broadcasts to short-form films, blogs, and amateur footage, particularly on YouTube. This transition has enabled amateur journalists to emerge as significant voices, so shaping a new epoch of citizen-driven public discourse.

Under the Obama administration, the United States enhanced its digital diplomacy strategies, implementing novel methods to engage global audiences and highlight concerns overlooked by mainstream media in many nations. These strategies occasionally undermined local authorities and converted internet agitation into tangible movements. The assertive digital engagement by the U.S. in the Middle East from 2009 to 2012 significantly influenced Russia, leading Russian entities to replicate, modify, and in certain instances intensify these strategies. Numerous analysts condemn Russia's digital diplomacy as ethically dubious characterized by cynicism and manipulation yet it has indisputably expanded the limits of social media's impact on global politics.

Not with standing extensive condemnation, Russian digital diplomacy has also provoked significant discussions. It has initiated an educational investigation on the impact of social platforms on public opinion and civilian engagement. In addition, it has inspired social media businesses to re-assure their moral and commercial standards. This essay will examine Russian information techniques (reference to Table 1) through strategic communication and public diplomacy lenses, and evaluate how these functions can be used by other states or non-state actors, regardless of moral views.

Table 1: Timeline of Russia's Digital Diplomacy (2000 2025)

Period	Key Developments
2000 2007	Initial diplomacy at the UN; promotion of global cyber norms begins
2008 2013	Cyberattacks on Estonia and Georgia raise concerns; SCO signs first information pact
2014 2017	Russia supports UN GGE norms; US-Russia cyber CBMs initiated
2018 2020	Push for cyber sovereignty; increased BRICS and bilateral digital treaties
2021 2025	Draft cybercrime treaty; pivot from West to Global South and China

Russia's Digital Diplomacy, early 2000s 2012: Looking for a Message and Target Audience

In terms of frequent tension between Russia and the West, it is important that in the early 2000s, Russia attempted to establish itself as a leader for generous development and democracy globally. During that period, Russia's public diplomacy served globally, as noted in 2008 by the Washington Post, that the nation was "clarifying its story of economic growth and opportunities for its citizens" and "to believe that the country [Russia] is a global player" (Washington Post, 2008). The primary objective during this period was to promote a positive perception of Russia globally, which targets the foreign community through cultural and informative initiatives. An example of this soft power campaign was the Cracking the Myth Documentary Series to a documentary series shown by Russia from 2007 to 2008. The series was designed to fight Russia's negative narratives, showing the claim of Russian aggression and imperialism as a baseless lie. Each program consisted of two sections: Russia's previous prevalent allegations, while the other intended to refute such critics. This

narrative technique uses a dialectical strategy, in which a bad proposal faces its opponent to achieve a more profitable end. The series aims to express a contemporary, progressive Russian identity for audiences worldwide by integrating scholars ' analysis of scholars, trends from ordinary Russians, and graphics showing the economic progress of Russia. This diplomatic campaign was fundamentally based on the concept of softening of Joseph Nyam, highlighting attraction and engagement as major equipment to shape international opinion.

Russia ultimately concentrated on two specific sectors of foreign people. The first group consisted of individuals with historical, cultural, or linguistic connections to Russia or the former Soviet Union. This encompassed a demographically varied group of individuals, differing in age, education, and political affiliation, who may still harbor favorable feelings towards Russia or nostalgia for Soviet principles. Russian-speaking consumers globally enjoyed uninterrupted access to media content in their own language, created and distributed from Moscow. In the subsequent years

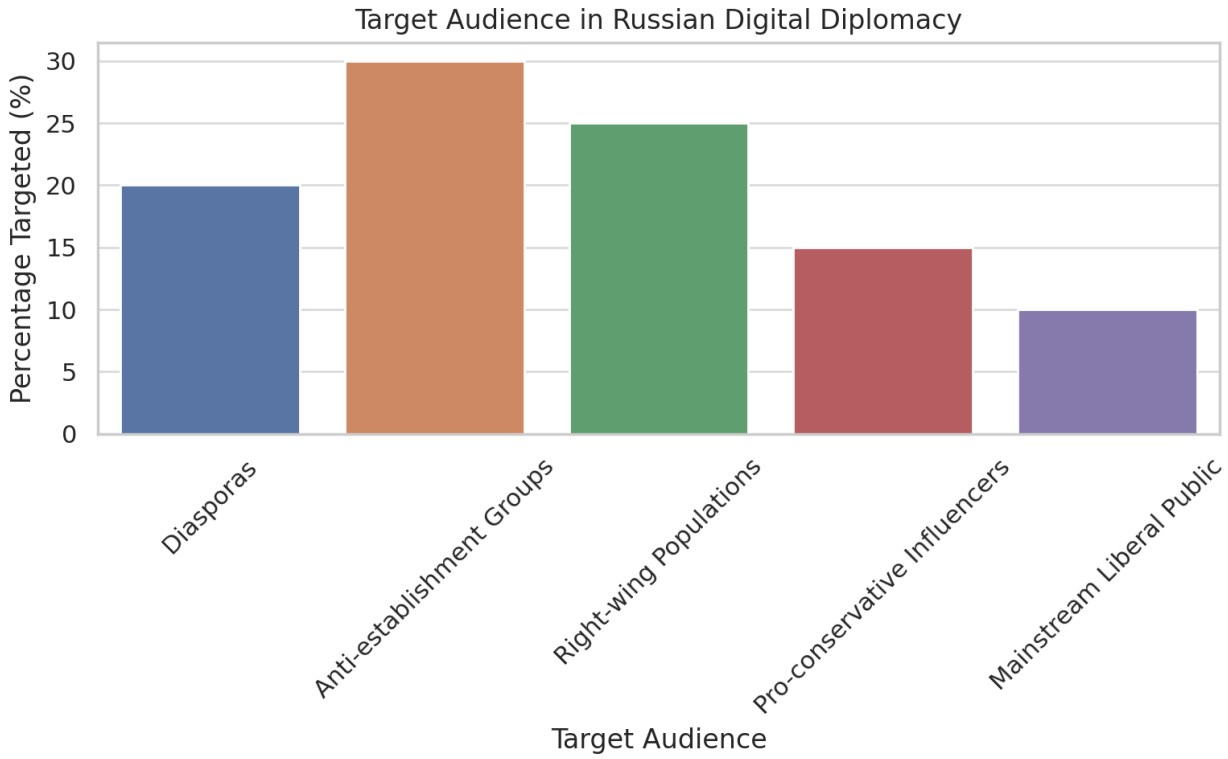

Fig 1: Target Audience Strategies A breakdown of audience targeting in Russia's digital diplomacy

Russia has markedly augmented its media power, currently generating almost 90% of news output aimed at Russian-speaking audiences—outpacing the historically predominant American and European broadcasters that formerly defined the worldwide Russian-language information sphere. In addition to this demographic, Russia has focused its public and digital diplomacy on a second group: individuals associated with both left-wing and right-wing movements who are disenchanted with mainstream media, political elites, and existing social frameworks in their respective countries. Table 2 and Figure 1 illustrate that Russia's strategy encompasses interaction with a diverse array of foreign political factions, frequently characterized by conflicting ideologies.

In contrast to other countries that generally focus on ideologically homogeneous audiences, Russia intentionally engaged both liberal and anti-liberal, leftist and rightist factions, exploiting their common dissatisfaction. This multipolar targeting significantly contrasts with Soviet-era

informational tactics, which primarily served pro-Communist and leftist audiences. In light of this ideological diversity, Russian communication necessitated a cohesive story that could resonate across a broad political and cultural spectrum (Tsvetkova, 2008). Effective public diplomacy relies on conveying a coherent, believable, and positive message. U.S. public diplomacy is founded on the principles of human rights, democracy, and freedom, establishing the nation as a global proponent of liberalism. Germany has highlighted innovation, comfort, and technological sophistication in its branding, as seen by its cultural diplomacy initiative "Germany – Land of Ideas." In contrast, Iran has promoted a narrative based on its heritage as a successor of Persian and Islamic civilization. The Soviet Union's exhortation to "Proletarians of all countries, unite!" equally resonated with international audiences sympathetic to communist beliefs. Conversely, early 2000s Russia faced challenges in developing a similarly persuasive narrative. The lack of a definitive, affirmative vision resulted in dependence on counter-narratives. Rather than highlighting its own advantages, Russian digital initiatives like "Question More" concentrated on revealing alleged deficiencies and contradictions within Western societies, offering alternative perspectives that align with Russian interests (Simons, 2015; U.S. House of Representatives Permanent Select Committee on Intelligence, 2018: viii). Between 2013 and 2018, Russian public diplomacy had a notable evolution, transitioning from ambiguity to clarity on its objectives, target audiences, and messaging. The updated emphasis highlighted a revitalized Russia with strategic economic and political aspirations extending from Eastern Europe to the Pacific. This transition signified a change from global image cultivation to the assertion of regional supremacy and strategic influence. Russia's revised digital diplomacy developed partially in reaction to perceived Western meddling—particularly American backing of liberal opposition factions within Russia and the instigation of "color revolutions" in adjacent nations. These developments, perceived in Moscow as strategic defeats, diminished the buffer zones historically deemed vital to Russian national security and incited a revanchist feeling within the Kremlin. Furthermore, the global media operations against Saddam Hussein, Muammar Gaddafi, and Bashar al-Assad demonstrated the Russian leadership the efficacy of offensive information warfare compared to defensive methods. Guided by these lessons, Russia embraced a more combative, forceful, and critical stance toward the West. The reformation of Russian public diplomacy encompassed both an ideological and a cultural transformation. Western lifestyles and values were increasingly depicted as dangers to Russian identity, government, and moral structures. As a result, a new narrative arose, rooted in conservative principles including the sanctity of the traditional family, religious values, and robust centralized governance. These themes constituted the foundation of Russia's worldwide communication and garnered significant appeal among conservative and anti-liberal audiences overseas (Simons, 2015a). This ideological shift signifies a distinct divergence from liberal soft power methods and highlights the conservative reconfiguration of Russian public diplomacy in the digital era.

Table 2: Target Audience Strategies in Russian Digital Diplomacy

Target Audience	Estimated Focus (%)
Diasporas	20%
Anti-establishment Groups	30%
Right-wing Populations	25%
Pro-conservative Influencers	15%
Mainstream Liberal Public	10%

Russia's Digital Diplomacy, 2013 2018: From Critics of Everyday life to Reality Show Campaigns in Target Countries

Since 2013, critics of the daily life and politics in target countries have shaped the agenda, goals, themes, and target groups of Russia's digital diplomacy. Russian international channels established alternative news to contest liberal narratives in the United States and Europe. The increase in political advocacy within Russia's international broadcasting has led to a focus on anti-capitalist, anti-liberal, and anti-U.S. sentiments, while simultaneously engaging with conservative, nationalistic, populist, and right-wing parties, thereby limiting its public diplomacy audience. Moscow commenced the use of its media to depict itself as a proponent of traditional values, juxtaposed against Western decadence. Putin's 2013 statement regarding Euro-Atlantic nations' rejection of Christian values and traditional identities has emerged as a strategic focus of contemporary Russian public diplomacy. Russia advanced the concept of a Russian World, characterized by a global culture rooted in traditional and conservative values. This initiative aimed to include individuals who held favorable views of Russia and communicated in the Russian language, thereby preserving its cultural identity. The Ukrainian crisis and the annexation of Crimea signaled a robust Russia asserting its influence over the Russian World. Russian information initiatives employed slogans such as "Russia defends Russians around the world," "the Russian World includes all individuals with cultural, linguistic, and historical ties to Moscow," and "Russia must safeguard its cultural and linguistic heritage globally" to rationalize the events in Crimea. A long-term foundation for Russian digital diplomacy has been established (Russia Today, 2015). Russian public diplomacy has consistently critiqued foreign politicians as well as social, economic, and political shortcomings. Russia has intensified its proactive and reactive propaganda campaigns on a daily basis. RT's advocacy campaigns disseminate provocative and potentially contentious information beyond the purview of Western media. The channel attracted a segment of the global audience that possessed anti-Western or pro-Russian perspectives. Julian Assange served as the host of the RT chat show "The World Tomorrow." The broadcast included interviews with anti-US organizations, featuring leaders from Hezbollah and various antigovernment parties globally, including those from Bahrain. Foreigners expressed enthusiasm for the Russian diplomacy project and participated in protest movements in the United States and Europe, including #Anonymous, #OccupyWallStreet, #OccupyChicago, and #Ferguson, which elicited alarm from mainstream news outlets in the US, UK, France, and other countries. The Occupy Wall Street documentary on RT depicted the movement as a struggle between the populace and the ruling elite. Corporations dominated the political landscape of the United States, with the White House serving as a tool for their interests. According to RT, revolutions, rallies, and protests have the potential to transform the US system. The dissemination of robust anti-US sentiment was a consistent strategy. Russian public diplomacy has reinvigorated Soviet-era propaganda techniques, promptly addressing critiques and unfavorable remarks regarding its foreign policy from the US and other nations through the use of whataboutism, exemplified by inquiries such as, "What about US foreign policy, relations with Iraq, protest movements, shootings, etc.?" In 2014, RT disseminated posters in various US cities to persuade Americans that the rationale for US military intervention in Iraq was rooted in falsehoods propagated by US media, encouraging them to visit RT.com for an alternative perspective (Tsvetkova, 2017: 249). The informational messages from Russia intensified during the period from 2015 to 2018. Russia has demonstrated an ability to portray truth in a negative context.

The documentary "Cultures of Protest" examines the US protest movement following Donald Trump's election, highlighting instances of violent political resistance. This documentary featured presentism, tone, and anti-mainstream perspectives that could challenge viewers' value consensus, despite the inclusion of some balanced facts. The West lacked preparedness for this form of Russian public diplomacy, which was perceived as aggressive propaganda. Mainstream media and experts have occasionally advocated for counter-information initiatives; however, the predominant narrative often perpetuates alarmist themes such as "Russians are coming" and "Russians are here." Digital diplomacy has recently concentrated on highlighting challenging themes and polarizing political issues. Digital programs produce polarized perspectives on significant issues and foreign adversarial profiles. Notable examples include Facebook posts expressing inflammatory views on LGBT issues, race, immigration, and gun rights in the United States (U.S. Senate Committee on the Judiciary, 2017). Russia is said to advocate for “Secured Borders” and “LGBT United” to sway American public opinion. The accounts advocate for varied values that stimulate discussions both online and offline. Social media enhances user engagement, which is leveraged by propagandists. Advertising directed at positive users reinforces their opinions and positions, prompting them to disseminate a message that exacerbates a problem (U.S. Senate Committee on the Judiciary, 2017). Posts on Facebook regarding "Secured Borders." Certain tweets addressed the need to secure US borders against illegal immigration, while others highlighted the pain, frustrations, and challenges faced by deported immigrants. The profile effectively illustrated both aspects of the issue; however, political disagreements exacerbated the conflicts surrounding the matters (U.S. House of Representatives Committee on Foreign Affairs, 2017: 22). The presence of multiple social media sources and profiles enhances the depth of problem discussions compared to reliance on a single source, profile, or account. A significant number of posts exhibit emotional content. Twin profiles featuring subtle title modifications and prominent hashtags such as #blacklivesmatter or #patriotic have led to an increase in followers and engagement, effectively disseminating a message. According to experts, Russia created between 120 and 470 American Facebook pages from 2015 to 2017 (The New York Times, 2017a). The U.S. Senate Committee on the Judiciary reported that 126 million Americans viewed over 80,000 posts on these pages, with 29 million engaging through sharing, liking, or commenting. The most frequented pages comprise “Blacktivists,” “United Muslims of America,” “Being Patriotic,” “Heart of Texas,” “Secured Borders,” and “LGBT United.” The discussion focused on contentious topics such as Muslim immigration, illegal immigration, liberal ideals, xenophobia, racial issues, and matters concerning sexual minorities. The Washington Post (2017) indicates that there are 9 million active conversations and responses across these six channels. YouTube and visualization have proven effective for disseminating information. YouTube serves as a significant influencer for foreign audiences. YouTube videos and footage are more effective in reaching users compared to bots and advertising or advocacy initiatives. Self-produced protest videos and independent journalist vlogs generate a perception of precision and exclusive information within social media feeds. YouTube has emerged as a significant source of news. American viewers constituted the majority of the audience for “RT America.” The channel boasts 800 million views on YouTube and 400 million followers, significantly surpassing engagement metrics on Facebook and Twitter (Office of the Director of National Intelligence, 2017). The majority of RT viewers engaged with its programming on YouTube rather than its television broadcast. Promoting a hashtag may further intensify divisions. Following the Arab Spring of 2010 2011, digital diplomacy has increasingly focused on hashtags, which can convey substantial information

regarding a situation. During that period, activists utilized hashtags to coordinate street protests. In 2011 and 2012, Russian protesters utilized hashtags, a practice that is now standard in digital campaigns. RT and other Russian digital diplomacy platforms disseminated WikiLeaks hashtags in their tweets, and this exchange occurred in both directions. The #podestaemails hashtag campaign disseminated an extensive analysis of former Secretary of State Hillary Clinton's presidential campaign, adversely affecting her reputation. Subsequently, it became evident that Twitter's administration inhibited the growth of hashtags in the summer of 2017 (U.S. Senate Committee on the Judiciary, 2017). Understanding the objectives, interests, and intentions of target audiences is essential for effective social media engagement. Digital diplomacy effectively addresses targets in contemporary contexts. Social media reconnaissance serves as a preferred approach for engaging and influencing individuals with similar ideologies. In previous years, social media networks provided accessible and comprehensive data regarding individuals, facilitating the selection of social media influencers. Facebook disclosed significant political preferences of key targets (U.S. Senate Judiciary, 2017). Until 2018, social media had the capacity to rapidly and effectively mobilize active users and the general public across various countries. This efficient mobilization focuses on specific issues related to Russia's favorable image, utilizing concise and engaging hashtags directed at targeted groups. Bots, as machine-driven communication tools, present a perspective aligned with their targets. Bots, rather than conventional international broadcasting, disseminate narratives to numerous users, generate thousands of tweets containing both accurate and inaccurate information along with hashtags, and elevate a hashtag to Twitter's trending list, thereby enabling authentic supporters to discover the narrative. Bots primarily distribute hashtags and topics that promote a nation's narratives directly into social media feeds. Digital diplomacy encompasses disclosure campaigns and doxxing practices. Digital diplomacy encompasses the use of hacking to acquire and disseminate confidential information with the intent to embarrass or undermine adversaries. The breach and data theft of the Democratic Party Committee server in August 2016 constituted a significant event of considerable impact. Correspondence involving Hillary Clinton, her aides, and Democratic Party leaders revealed unethical political practices that compromised her credibility. Political campaigns in various nations may employ doxxing against opponents, thereby increasing the potential for multiple entities to influence foreign elections. Innovative hashtags and videos may provoke a significant number of social media users to resist mainstream media's attempts to mitigate the situation. The English-language RT video titled “Julian Assange Special: Do WikiLeaks Have the E-mail That’ll Put Clinton in Prison?” contributed to the proliferation of anti-Hillary Clinton sentiment (Russia Today, 2016). Reality show campaigns that promote public engagement represent a significant and potentially the most effective digital strategy. The most notable and widely reported case was the “vote-by-text Tweets” campaign, which prompted American users to vote through SMS and tweets rather than at polling centers. Supporters and opponents of the Texas Muslim library engaged in street protests following a misleading social media campaign. International digital diplomacy could draw on instances from Russia (U.S. Senate Committee on the Judiciary, 2017; The New York Times, 2017b). The integration of bots, transparency measures, and offline initiatives has enhanced digital diplomacy. Machines will undoubtedly acquire target audiences. Experts from America and Europe concur that artificial intelligence and digital diplomacy will enhance public diplomacy (Department of State, 2017). A robot has the potential to generate thousands of comments and impact millions through precise and persuasive responses.

Russia's Digital Diplomacy, 2018 2025

Russia's diplomatic posture in cyberspace evolved markedly after 2018 as shown in table 3 and fig 2. Initially Moscow engaged tentatively with Western partners, but analysts note a decisive pivot following the Ukraine conflict. Chernenko (2024) observes that after a brief mid-2021 cyber "détente" with the U.S., Russia "shifted its focus towards non-Western countries and alliances". This reflects a broader pattern: Russia's leaders have long distrusted Western-driven cybersecurity frameworks and instead built regional coalitions. For example, Russia emphasized *cyber sovereignty* at the United Nations, opposing the liberal multi-stakeholder model favored by the U.S. and EU (Epifanova, 2020). In practice, Russia reoriented its digital diplomacy from global forums toward friendly states and blocs (BRICS, SCO, CSTO), framing these as cooperative alternatives to Western initiatives.

Table 3: Growth of Russia's Cyber Treaties and Agreements (2010 2025)

Year	Number of Treaties Signed
2010	1
2011	2
2012	3
2013	4
2014	4
2015	6
2016	7
2017	7
2018	8
2019	9
2020	10
2021	12
2022	13
2023	14
2024	14
2025	15

Russia pursued multiple new initiatives on the cyber/information-security front during 2018 2025. Key examples include:

- **Bilateral information-security agreements:** In 2022 Russia signed intergovernmental pacts on "security in the information space" with Armenia and Azerbaijan, and in 2023 with Zimbabwe (PIR Center,). These treaties establish legal frameworks for joint cyber-incident response and capacity-building, officially aimed at countering shared "threats in the information space".
- **BRICS and allied partnerships:** At the 2022 BRICS summit (Beijing), members launched a *Digital Economy Partnership Framework* to promote cooperation on e-commerce, data protection, and cybersecurity (Council on Foreign Relations, 2023) . This multilateral effort reflected in the official BRICS declaration aligns with Russia's goal of forging a non-Western digital governance bloc.

- **Russia China cyber cooperation:** During President Putin's March 2023 visit to China, a joint statement pledged support for a "multilateral, equitable and transparent global Internet governance system" that ensures each country's sovereignty and security (Atlantic Council, 2023). Both sides also endorsed work on new international cyber norms and a possible treaty on information security, signaling coordinated diplomacy on this issue.
- **UN and global forums:** Russia has used the UN to advance its vision of cyber norms. It sponsored a 2018 UN General Assembly resolution on international information security, and in 2023 submitted a draft "Convention on International Information Security" to the UN Open-Ended Working Group. Western analysts warned that this draft could "undermine accountability of state actions in cyberspace", since Russia's proposal stressed sovereignty and non-interference in ways that critics say legitimize state surveillance and censorship. (Many countries pointed out that existing law already applies in cyberspace, rejecting Russia's claim of legal "gaps" (Manor, 2021).

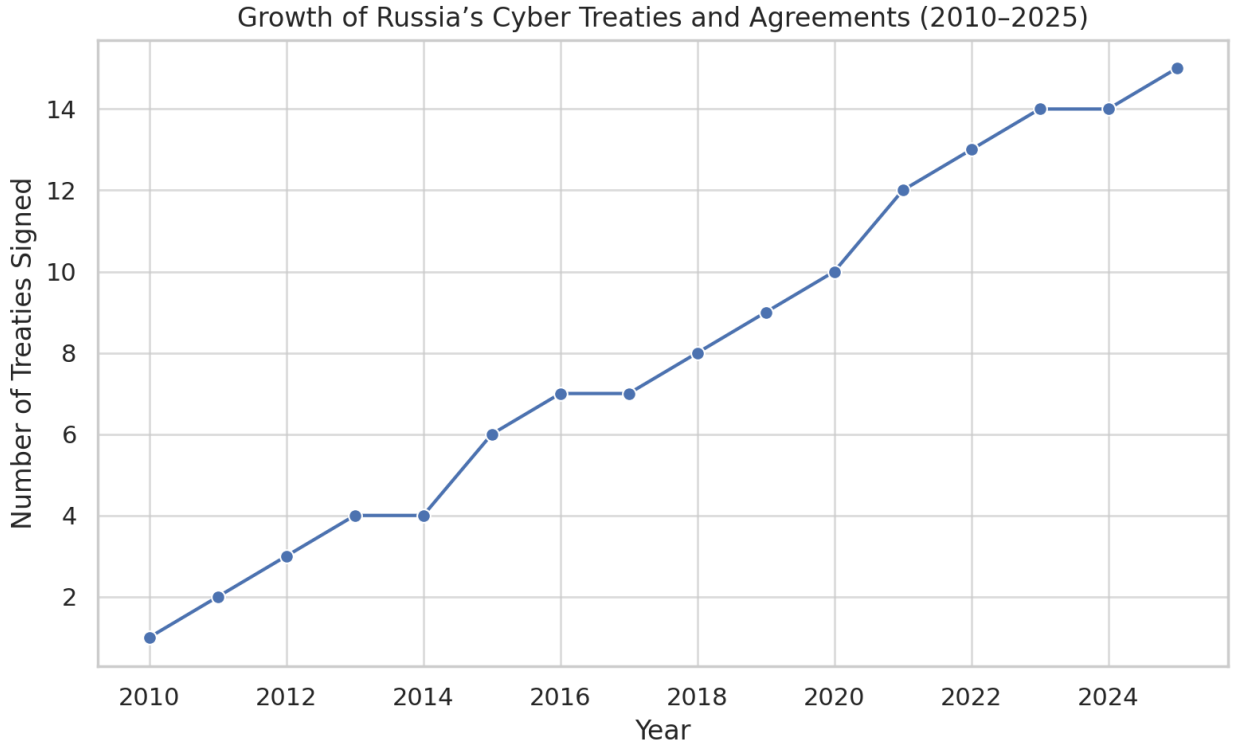

Fig 2: Cyber Treaties Growth A year-wise trend in signed cyber agreements

Domestically, Russia enacted policies reinforcing its international stance on digital sovereignty. Notably, the 2019 2020 "sovereign Internet" law requires Russian ISPs to install state-controlled filtering equipment and establishes a national DNS, in theory enabling the government to isolate the Russian network from the global Internet. Epifanova (2020) explains that these amendments create a legal framework for centralized state management of Russia's Internet, which is likely to "accelerate fragmentation of the global internet". Russia has also expanded strict data-localization rules (mandating foreign platforms to store Russian users' data on local servers) and tightened online content controls. Analysts argue that under these laws together with wartime sanctions "digital technological isolationism" has become a deliberate Kremlin objective. Sherman (2024) observes that such policies have made the push for "digital sovereignty" explicit, noting that it is

now “both a reality and a desired goal for Moscow”. In practice this has driven greater reliance on domestic and allied (particularly Chinese) technology in Russia’s digital infrastructure.

Disinformation and influence operations have been central to Russia’s state-backed digital outreach. State media outlets (RT, Sputnik, etc.) and coordinated online troll networks have spread false narratives aimed at foreign publics. As the Atlantic Council’s Digital Forensic Research Lab reports, Russia “remains fully committed to conducting information operations around the globe” (Atlantic Council, 2023). These operations have targeted Western audiences, non-aligned regions, and countries in Russia’s near abroad. In the lead-up to Russia’s 2022 invasion of Ukraine, Russia waged intense “narrative warfare” crafting stories to justify its actions, mask its military plans, and shift blame onto Ukraine. After the invasion, when Western sanctions curtailed state-media reach in Europe, Russia “adjusted its information operations to focus more on social media” and expanded propaganda campaigns into Latin America, Africa, and the Middle Eastatl, aiming to erode support for Ukraine globally. These aggressive influence efforts complement Moscow’s official e-diplomacy: Manor (2021) notes that Russian embassies’ social-media accounts actively tailor messaging to local contexts, “resonating with local narratives” and using historical references to justify current Russian policy. In short, Russia’s digital diplomacy encompasses both overt engagement (embassy outreach) and covert disinformation campaigns, reflecting a fusion of traditional public diplomacy and information warfare.

Table 4: Comparative Cyber Norm Positions (Russia, US/EU, China)

Issue	**Russia**	**US/EU**	**China**
Cyber Sovereignty	Strongly Supports	Opposes	Supports
Multistakeholder Governance	Opposes	Strongly Supports	Mixed
Preference for Binding Treaties	Supports	Opposes	Supports
Use of Information Operations	Extensive	Limited	Extensive
Support for UN Cybercrime Treaty	Leads	Cautious	Supports

Russia’s cyber-diplomatic model has met persistent criticism as shown in table 4 . Western analysts and human rights supervisors have warned that the Internet regime based on Moscow's "sovereignty" effectively prohibits powerist control. For example, Valentin Weber (2020) argues that these measures effectively "provide validity to state monitoring and censorship". Similarly, policy commentators take precautions that Russia's new internet-control law will speed up a "splinton" in the internet balconies that fractures global connectivity. Many states also look at Russia's international proposals with doubts: after the 2023 treaty draft, critics reported that it could weaken the existing accountability mechanisms and strengthen oppressive norms. Overall, the observers note that while Russia presents its cyber diplomacy as stability and promoting mutual security, in practice, it deepens distrust between cyber powers. By prioritizing unilateral sovereignty and creating parallel regional institutions, Russia's perspective has widened the difference between East and West on cyber issues and formed a consensus on global norms that are rapidly elusive.

Conclusion

This research has detected the important role of diplomacy in shaping international cybersecurity. Russia has served as a hypothetical case study due to its complex, developed, and often controversial situation within the global cyber regime landscape. It is clear through a multi-

theoretical lens that incorporates realism, liberalism, and compositionism that cyber diplomacy not only serves as a strategic tool to protect national security interests, but also serves as an ideal platform to present an impact and competing stories in an election-fighting digital environment.

In the last two decades, there has been a fundamental change in Russian digital diplomacy. Initially characterized by abstract appeal to global inclusion in the early 2000s, Moscow's digital outreach was suffering from unclear purposes, strategic messages, and an undefined target audience. These deficiencies reflected wide ambiguity in Russia's post-Cold War Foreign Policy. However, by 2013, this approach was replaced with more vocal and ideologically harmonious models. With a view to restoring a conservative political turn and geopolitical impact, Russia's digital diplomacy shifted both in the domestic and abroad, marginalizing and targeting disgruntled communities. In fact, Russia has given the U.S. and led by the European Union, but has renovated itself to serve its specific strategic goal.

Russia's digital diplomacy, especially from 2018 to 2025, strengthened its role as a prominent actor in international cybersecurity diplomacy. The state actively pursued bilateral and multilateral partnerships with non-Western countries, engaged in advanced sovereignty-based cyber norms in the United Nations. It employed a layered communication strategy involving both traditional diplomacy and information operations. It maintained a formal participation in global forums such as the UN Open-Ended Working Group and Cybercrime Treaty Dialogue, exploited and innovated in all liberal democratic institutions, enhancing social media algorithms, enhancing armed fringe stories, and enhancing and innovating frozen stories.

Importantly, this dual-track strategy lies in formal diplomatic channels and redefined the shape of global digital engagement in disruptive effects operations in another. Russia's active role has worried Western governments and inspired the global revaluation of transparency, content regulation, and digital flexibility. The country has contributed to a new public consciousness of how social media can be made weapons, and how diplomacy should suit the mobility of the information age itself. In doing so, Russia has not only vocal itself as a cyber power, but in many ways, earned the status of a "digital empire", which deeply influences how nations now concept and implement the concept of digital diplomacy.

Finally, Russia's case underlines a fundamental reality of 21st-century diplomacy: Cyberspace is no longer a peripheral domain, but a central region of geopolitical competition and cooperation.Cyber diplomacy whether manifesting as treaty advocacy, norm entrepreneurship, or strategic disinformation has become a core component of statecraft. As cyber threats continue to evolve, the international community must embrace a balanced approach that integrates security imperatives with inclusive, transparent, and rights-based frameworks. Russia’s trajectory offers critical lessons: the power of narrative, the utility of hybrid strategies, and the enduring importance of diplomacy even amidst digital disruption. To foster a safer, more stable cyber environment, diplomatic engagement must remain resilient, adaptive, and grounded in both principled dialogue and pragmatic cooperation.

Reference

1. American Foreign Service Association. (n.d.). *Cyber diplomacy for strategic competition*. https://afsa.org/cyber-diplomacy-strategic-competition#:~:text=Cyber%20diplomacy%20is%20the%20use,of%20digital%20technologies%20and%20trade

2. Arbatov, A., & Oznobishchev, S. (Eds.) (2016). *Russia: Arms Control, Disarmament and International Security, IMEMO Supplement to the Russian Edition of the SIPRI Yearbook 2015*. Moscow, p. 98
3. Atlantic Council. (2023). *Russia's Digital Tech Isolationism: Domestic Innovation, Digital Fragmentation, and the Kremlin's Push to Replace Western Digital Technology*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-digital-tech-isolationism/
4. Ayodele, O., & Petla, V. (2024). *Leveraging the BRICS Digital Partnership for Collaborative Digital Governance*. *Journal of BRICS Studies*, 3(1). University of Johannesburg Press. https://journals.uj.ac.za/index.php/jbs/article/view/2485
5. Bubnova, N. (Ed.) (2011). *20 Years Without the Berlin Wall. A Breakthrough to Freedom*. Carnegie Moscow Centre, pp. 187–216
6. Bubnova, N. (Ed.) (2012). *World in Their Hands: Ideas From the Next Generation*. Carnegie Moscow Centre, pp. 187–216
7. Chernenko, E. (2024). *The Future of Strategic Stability and Arms Control Were Discussed at the 122nd Summer Session of the Trialogue Club International*. PIR Center. https://pircenter.org/en/news/the-future-of-strategic-stability-and-arms-control-were-discussed-at-the-122nd-summer-session-of-the-trialogue-club-international/
8. Chernomorova, T.V. (2015). *The Image of Russia Created by the British Press (in Russian)*. Russia and the Contemporary World, 2(87), pp. 184–198
9. Clinton, H.R. (2014). *Hard Choices*. Simon & Schuster, London
10. Council on Foreign Relations. (2023, March 7). *The Dangers of a New Russian Proposal for a UN Convention on International Information Security*. https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security
11. Council on Foreign Relations. (n.d.). *Increasing international cooperation in cybersecurity and adapting cyber norms*. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms#:~:text=There%20is%20an%20urgent%20need,Emerging%20cyber%20threats%20could
12. Dong, J., Chen, S., Ding, F., et al. (2025). Spatiotemporal characteristics and drivers of global cyber conflicts. *Humanities and Social Sciences Communications, 12*, 665. https://doi.org/10.1057/s41599-025-04897-7
13. Epifanova, A. (2020). *Deciphering Russia's "Sovereign Internet Law"*. German Council on Foreign Relations. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law
14. Epifanova, A. (2020). Deciphering Russia's "sovereign internet law". *DGAP Analysis No. 2*. German Council on Foreign Relations. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law#:~:text=In%20November%202019%2C%20Vladimir%20Putin%E2%80%99s,Russian%20reliance%20on%20Chinese%20technology
15. Epifanova, A. (2020). *Deciphering Russia's "Sovereign Internet Law"*. DGAP Analysis 2. German Council on Foreign Relations. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

16. Feffer, J. (2018). *Call It "Unileaderism": Trump's Foreign Policy of One*. Foreign Policy in Focus
17. Finkel, E. (2011). *In search of "lost genocide" (in Russian)*. Pro & Contra, 3–4(52), Carnegie Moscow Centre, pp. 123–143
18. FutureBrand (2016). *Country Brand Index 2014–2015*. https://www.futurebrand.com/uploads/CBI2014-5.pdf
19. Jones, J.M. (2018). *More in U.S. Favour Diplomacy Over Sanctions for Russia*. Gallup
20. Kagan, R. (2006). *Dangerous Nation. America's Place in the World from Its Earliest Days to the Dawn of the Twentieth Century*. Alfred Knopf, New York
21. Kasyanov, G. (2009). *Ukraine: Holodomor and nation building (in Russian)*. Pro et Contra, Politics of History, 13(3–4), pp. 24–42
22. Kortunov, A. (2016). *When interpreting Putin's actions, don't take nostalgia for ambitions (in Russian)*. Russian International Affairs Council
23. Korzak, E. (2021). Russia's cyber policy efforts in the United Nations. *Tallinn Paper No. 11*. NATO Cooperative Cyber Defence Centre of Excellence.
24. Kurowska, X. (2019, December 18). What does Russia want in cyber diplomacy? A primer. *EU Cyber Direct*. https://eucyberdirect.eu/research/what-does-russia-want-in-cyber-diplomacy-a-primer
25. Manor, I. (2021). *Russia's Digital Diplomacy: The Good, the Bad and the Satirical*. Russland-Analysen, (398). https://doi.org/10.31205/RA.398.01Korea Science+1kapdnet.org+1
26. Manor, I. (2021). *What Are the Future Challenges for Digital Diplomacy?* Exploring Digital Diplomacy. https://digdipblog.com/2021/09/09/what-is-are-the-future-challenges-for-digital-diplomacy/
27. McClory, J. (Ed.) (2016). *The Soft Power 30: A Global Ranking of Soft Power*. Portland, London
28. McGann, J.G. (2018). *2017 Global Go To Think Tank Index Report*. University of Pennsylvania
29. National Security Strategy of the United States of America (2017). *December*. , P. II, P.1., P.2.
30. Nye, J.S. (1990). *Soft Power*. Foreign Policy, 80, pp. 153–171
31. Obama, B. (2006). *The Audacity of Hope. Thoughts on Reclaiming the American Dream*. https://archive.org/stream/TheAudacityOfHope_201607/...
32. PIR Center. (n.d.). *Chapter 8. Russia's Cyber Diplomacy: A Change in Progress*. Security Index Yearbook. https://pircenter.org/en/editions/security-index-yearbook-chapter-8-russia-s-cyber-diplomacy-a-change-in-progress/
33. PIR Center. (n.d.). Chapter 8. Russia's cyber diplomacy: A change in progress. *Security Index Yearbook*. https://pircenter.org/en/editions/security-index-yearbook-chapter-8-russia-s-cyber-diplomacy-a-change-in-progress/#:~:text=Over%20the%20past%20two%20years,Western%20world
34. Segal, A. (2023, August 15). The sinicization of Russia's cyber sovereignty model. *Council on Foreign Relations*. https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model#:~:text=While%20all%20states%20would%20claim,importantly%2C%20the%20resolution%20created%20an

35. Sherman, J. (2024). *Confronting Russia's Cyber Power: Reassessing Assumptions, Sizing Up the Threat, and Building a Proactive Response*. Atlantic Council. https://www.atlanticcouncil.org/event/report-launch-confronting-russias-cyber-power/
36. Sherman, J. (2024). Russia's digital tech isolationism. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-digital-tech-isolationism/#:~:text=1,well%20as%20its%20efforts%20to
37. Shestopal, E., & Smulkina, N. (2018). *How Do Russians Perceive Their Country Today (in Russian)*. Politeia, 2(89), pp. 51–68
38. Simes, D. (1999). *After the Collapse*. New York, pp. 15–20
39. Simons, G. (2016). *Post-Soviet Geopolitics in the Age of the New Media*. In Suslov, M. & Bassin, M. (Eds.), Eurasia 2.0, pp. 275–294
40. Simons, G. (2018). *Media and Public Diplomacy*. In Tsygankov, A. (Ed.), Routledge Handbook on Russian Foreign Policy, pp. 199–216
41. SIPRI Yearbook (2015). *Armaments, Disarmament and International Security*. Russian edition (IMEMO RAN), pp. 155–156
42. Snyder, T. (2018). *The Road to Unfreedom. Russia, Europe, America*. Penguin Random House,
43. Spring 2017 Global Attitudes Survey (2017). **. Pew Research Centre,
44. Spring 2018 Global Attitudes Survey (2018). **. Pew Research Centre
45. Stokes, B. (2015). *Russia, Putin Held in Low Regard around the World*. Pew Research Centre
46. Sustainability Directory. (2025, March 17). *International cyber security*. Climate Sustainability Directory. https://climate.sustainability-directory.com/term/international-cyber-security/#:~:text=,stable%20cyberspace%20for%20all%20nations
47. Weber, S. (2023). *Thinking About Long-Term Cybersecurity: A Conversation With Steven Weber and Betsy Cooper*. Council on Foreign Relations. https://www.cfr.org/podcasts/thinking-about-long-term-cybersecurity-conversation-steven-weber-and-betsy-cooper
48. Wike, R., Stokes, B., Poushter, J., & Fetterolf, J. (2017). *U.S. Image Suffers as Publics Around World Question Trump's Leadership*. Pew Research Centre
49. Yegorov, O. (2016). *Russia Ranks Among Top 30 Countries Worldwide in Terms of Soft Power*. Russia Beyond the Headlines, 15 June
50. Zinovieva, E. (2023, May 22). International information security in US-Russian bilateral relations. *Modern Diplomacy*. https://moderndiplomacy.eu/2023/05/22/international-information-security-in-us-russian-bilateral-relations/#:~:text=Amid%20a%20complex%20geopolitical%20environment%2C,nations%20in%20the%20long%20term