P-ISSN: 2709-6254	Journal of Development and Social Sciences	Jan-Feb 2026, Vol. 7, No. 1
O-ISSN:2709-6262	https://doi.org/10.47205/jdss.2026(7-I)01	[01-10]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Cyber Warfare and Digital Competition between US and Russia: A Comparative Analysis Cyber Policies and Strategies

[1]Hafsa Javed, [2]Ayesha Javed and [3]Bisma Seerat

1. MS Scholar, Department of Politics & IR, GC Women University Sialkot, Punjab, Pakistan
2. MS Scholar, Department of Politics & IR, GC Women University Sialkot, Punjab, Pakistan
3. MS Scholar, Department of Politics & IR, GC Women University Sialkot, Punjab, Pakistan

Corresponding Author: hafsajaved786123@gmail.com

ABSTRACT

The objective of this Study is to relatively examine the cyber warfare strategies and virtual competition policies of the United States and Russia. It aims to focus on comparative analysis of cyber policies and strategic intentions shaping their cyber techniques.Cyber warfare has emerged as a vital domain of present day international security and power opposition. Both America and Russia view cyberspace as a strategic area for influence, deterrence, and war without conventional conflict. Their cyber strategy is vital to assess worldwide digital security dynamics and geopolitical balance.This study adopts a qualitative comparative analysis primarily based on secondary Sources, such as policy documentsUS, legit reviews, and scholarly literature.The findings reveal that the USA emphasizes protecting resilience and international norms, even as Russia makes a speciality of offensive cyber skills and data struggle. Both countries actively combine cyber equipment into their broader country wide protection strategies.The study recommends strengthening worldwide cyber norms, enhancing cooperation on cyber security, and selling self belief building measures to reduce escalation dangers.

KEYWORDS Cyber Warfare,United States, Russia, Cyber Policies ,Cyber Strategies

Introduction

Cyber warfare means using computers ,digital technology and the internet to attack or harm other countries. Cyber War has emerged as a critical dimension to reshaping the States ,compete and Defend in the digital age.The concept of cyber warfare began when countries depend on computers ,the Internet and digital technology.Instead using a weapon, cyber warfare targets computer data and networks. In the traditional Era no functions of computers and internet .States were fought for the defence of their country through Sword and other physical weapons. Traditional wars organised by military forces of different domains yearn for naval and land forces. Conventional war had a sincerely described beginning and end given the distinction between Warfare and peace was more visible than in modern conflicts.

Cyberwarfare among Russia and the United States has evolved specially because the early 2000s have an effect on operations and infrastructure probing rather than open digital war. First occasions encompass Russian related cyber activities inclusive of the 2007 assaults on Estonia,the 2014–2016 intrusions into U.S. authorities systems, and the interference within the 2016 U.S. presidential election through hacking and facts operations attributed by U.S. intelligence to Russian actors. In reaction, the United States has acknowledged carrying out its own cyber operations, along with offensive cyber competencies below U.S. Cyber Command, aimed toward deterrence and disruption of adversary networks. America and Russia, as major worldwide powers, have developed advanced cyber skills reflecting their strategic priorities. The United States has historically emphasized offensive cyber operations. On the other hand Russia prioritizes information disagreement, digital sovereignty, and hybrid techniques .

This examination compares the cyber policy framework ,doctrine and strategic practice of both international states. It examines how every state perceives cyber threats and possibilities ,implements national cyber policy and competes in digital technologies for strategic advantage .Moreover, comparative analysis of cyber policies and cyber warfare permits policymakers and protection experts to pick out variations in strategic priorities and Policies.

Literature Review

Cyber warfare extensively described in Nations sponsored operations that use virtual tools to affect any other country structures Infrastructures are record surroundings.Scholars that cyber operations blur the difference between peace time opposition and war.Although cyber warfare literature on America and Russia is large, there is a clear gap in systematic, side by aspect comparative research that links professional cyber policies with actual operational practices. Most studies analyze each U.S. separately, with a restricted exam of the policy practice gap, in particular concerning transparency, prison norms, and strategic intent. Moreover, the position of rising technology together with AI and automated cyber operations remains underexplored in comparative analyses, restricting expertise of how digital opposition between the U.S. and Russia is evolving.A single nicely orchestrated cyber assault can potentially paralyze vital infrastructure, disrupt financial structures, and compromise countrywide protection mechanisms. The asymmetric nature of those conflicts means that traditional deterrence techniques become ineffective, developing a new paradigm of worldwide strategic engagement (Shahbaz & Muzaffar, 2025; Khan, 2025).

The internet has added people and services together by making records exchange less complicated and faster. However, despite that fact's value, those services have ended up a target of cyber threats, and these threats are a mission to defeat. Malicious attacks are reasonably priced, easy and regularly pose little chance in terms of attribution , however their effect is good sized . Not tremendously, this has led many governments to develop businesses and policies designed to improve cyber defense. The multiplied emphasis in cyber-associated policy is nicely located, but effectiveness has to be assessed empirically (Kumar, 2016).

Cyberwarfare has now entered a third wave with the introduction of artificial intelligence (Al) which has led to the rebellion called the third revolution in army affairs (Thornton & Miron, 2020).

The research factors out the efforts of the U.S. and Russia to apply Al to predictive modeling of threats. The U.S. Cyber Command (USCYBERCOM) is said to incorporate Al to shield the important infrastructure, perform penetration testing, and mimic the movements and responses of adversaries (Schaub & Maurer, 2021).

Despite the fact that, the identical researchers warn additionally on the acute use of a self reliant system. consistent with Binnendijk (2020), the diagnosed risks consist of escalation because of false positives or misunderstanding the character of the incident by way of an Al in the instances of ambiguous cyber incidents. The moral aspects of self sufficient cyber responses aren't fully developed inside the U.S. doctrine, evoking issues approximately the obligation in the Al-improved (Khalid,2025; Yaseen, Muzaffar, & Aman, 2022). The United States of America has an intelligence network that leads in identifying and publicly exposing cyberattack perpetrators to eliminate their anonymity (America, 2018, p. eleven). The events of cyber attacks like Estonia ,Georgia ,Ukraine, Presidential election of U.S (2016).

Material and Methods

This study adopts a qualitative comparative research design to research cyber policies inside the context of cyber warfare. .Information is accrued from primary sources, consisting of authentic cyber coverage files and country wide safety techniques, and secondary assets together with educational journals, books, assume-tank reports, and credible news articles. The statistics is analyzed through content and comparative analysis, identifying key subject matters inclusive of offensive and defensive cyber techniques, cyber sovereignty, and worldwide cyber norms.

Results and Discussion

The US has long past an extended manner in incorporating Al in its protection/Cyber infrastructure. The Joint synthetic Intelligence center (JAIC) of the U.S. department of protection became created in 2018 to manipulate the improvement of Al among offerings. Project Maven is one of the examples to reveal that the U.S. is aimed toward using Al to research intelligence and prioritize objectives (Allen & Husain, 2017).

Russia its conceptualization strategic files like the country wide safety approach (2015) and records security Doctrine (2016).The Russian time period for 'cyber conflict' is 'records technological battle', which is part of the wider idea of 'records disagreement' (informatsionnoe protivoborstvo).Russian army thinkers use the time period 'cyber' for Western threats but keep away from linking it to their very own talents because of negative Soviet technology connotations and the importance of 'data protection' in home politics.'facts area' (informatsionnoe prostranstvo) or 'information sphere' (informatsionnaya sfera) is extra complete than the Western 'cyber area'. Development in Digital technologies and deployment of AI structures has now enabled developing deepfakes, digital competitions ,automating disinformation campaigns, and influencing mass opinion in approaches that one ought to have by no means imagined before (Guyonneau & Le Dez, 2019).Cyber operations using IA have given more desirable competencies including adaptive, self sufficient, and predictive. In other words, vulnerability detection and exploit deployment has now grow to be potential in actual-time with gadget getting to know (Hallaq et al., 2017: Timilehin, 2023), bringing each the attacker and defender into a whole lot nearer interplay with each other. Al-superior offensive cyber weapons are gaining extra capabilities in self sustaining discovery, malware development and adversary subversion, while Al is being used at the protecting facet to boom resilience via anomaly detection and predictive modeling (Gabrian, 2024; Shoaib, 2016).

Russia's strategic deterrence extends past nuclear and conventional military electricity to encompass a wide array of non-military gear, including ideological, political, diplomatic, wireless, and informational measures.the overall aim of information confrontation is to gain strategic consequences and beware wireless superiority over combatants, frequently in peacetime, without triggering direct army conflict.

Russian and US Cyber Policies

Russia's policy on international information security defines this as a worldwide records space where global peace and safety are ensured through diagnosed legal principles and identical partnership, considering countrywide pursuits. The policy's cause is to set up a prison regime to save you interstate conflicts inside the international information area and shape a safety gadget. Key individuals supposed to cooperate include the Commonwealth of impartial States (CIS), BRICS, the Collective safety Treaty organization (CSTO), the Shanghai Cooperation organization (SCO), and the affiliation of Southeast Asian countries (ASEAN). The policy ambitions to make certain safety through reducing or removing threats, specially figuring out six threats, along with undermining navy-political standpoints, violating sovereignty, and facilitating terrorist assualts.Terrorist assaults, together with propaganda and recruitment.Extremist interference with internal affairs of sovereign states.Cyber-crimes, which include various types of fraud.Cyber-attacks in opposition to vital information

infrastructure.The policy also includes developing overseas members of the family to decorate global facts security. The supply is identified because of the 2021 "fundamentals of the country policy of the Russian Federation in the area of worldwide records safety. The Russian Federation's coverage for enhancing international data protection via foreign members of the family and cooperation. The primary goal is to establish a democratic, inclusive, and transparent negotiation method concerning facts and verbal exchange technologies. The policy emphasizes selling peace and pleasant relations and information specific implementation strategies and solutions to diverse threats, such as preventing the undermining of navy political sovereignty, counteracting terrorist attacks, monitoring extremist interference, decreasing cybercrimes, protecting crucial statistics infrastructure, and preventing marketplace monopolization.

Setting up the worldwide Cyber Deterrence Initiative to coordinate and jointly impose effects (sanctions, indictments) on adversaries .Legislative modernization running with Congress to replace digital surveillance and pc crime laws to enhance regulation enforcement abilities.Investment in step forward technologies Prioritizing the development and deployment of quantum resistant cryptography, SG, and synthetic intelligence to hold technological leadership .combating disinformation using all available equipment to reveal and counter overseas have an effect on campaigns on line (u.s.a., 2018, p. 11).Allies and companions America correctly operationalized its coalition-constructing mandate, extensively via the coordinated expulsion of Russian intelligence officers in 2018. greater than 60 Russian officials, along with 48 diplomatic personnel, were expelled, and the Russian consulate in Seattle changed into closed in response to the poisoning of Sergei Skripal (U.S. branch of country, 2018).

Russian Cyber Strategy

Russian Cyber strategy includes , Russian national security,information warfare strategy ,military strategy and cognitive warfare strategy. These tactics focus on defending national security objectives ,maintenance of operational superiority ,accomplishing strategic aims and reinforcing cyberspace .

Russia's national security strategy, applied in July 2021, outlines the kingdom's approach to defending its domestic and worldwide pastimes. The strategy ambitions to safeguard sovereignty, territorial integrity, and countrywide hobbies across political, financial, social, navy, and informational spheres, even as improving resilience to internal and outside threats. members, together with government businesses, protection offerings, army forces, and citizens, analyze threats and broaden countermeasures. Implementation includes an in depth movement plan with precise timelines, responsibilities for relevant government agencies just like the FSB and SVR, and mechanisms for monitoring progress through ordinary reporting and protection Council conferences.

Russia Military Strategy

Russia's military approach aims to put together a continuous struggle, shield its superb electricity fame, and adapt to rising navy doctrines. The strategy specializes in preserving deterrence, executing operations concentrated on critical infrastructure, and stopping fighters from attaining early decisive victories. Key techniques involve leveraging navy techniques for political targets, the use of precision-guided guns, using non-kinetic assaults, and disrupting opponent command structures. Implementation plans include readiness demonstrations, sporting activities, emphasizing offensive processes, and adapting to changes in struggle.

Russia's strategy on cyber operations and facts struggle, emphasizing its aim to reap countrywide pastimes and political objectives through persistent exploitation of the cyber domain .To strengthen Russia's global position and promote strategic balance in

reaction to perceived containment with the aid of the United states and its allies. objectives consist of undermining enemy infrastructure, swaying public opinion, carrying out espionage, and gaining geopolitical gain.Russia's approach for cyber operations and records struggle, which employs non-traditional and asymmetric methods to attain deterrence and constraint. Russia has developed a strategy for cognitive warfare and psychological manipulation, obvious in its cyber operations during the last many years. This method aims to manipulate cognizance in present day and destiny navy conflicts.

The strategy includes using technology together with data pressure, hacker attacks, and cyber warfare to influence the overall populace.scientific business bases improvement of Russian produced hardware and software programs for protection and navy use.Blacklisting and content material management Targeted surveillance systems Centralized localization and retention of statistics wi-fi by way of internet provider carriers (ISPs) for counterintelligence, regulation enforcement, and political control.Safety of essential facts Infrastructure (CII) big prison regimes based on kingdom ownership manipulation, inclusive of backups of DNS and IXP, allowing disconnection from the worldwide community.Facts-technological and facts-psychological countermeasures control through nation managed media and educational patriotic institution.To make sure safety from internal and external statistics threats by setting up an independent Russian internet. Home security is supported by using structures like SORM (System of Operative-search Measures) and GosSOPKA.SORM, a surveillance technology permitting the tracking of phone and internet wireless, which include metadata and content. Net carrier carriers (ISPs) are legally obligated to put in probes for the Federal protection service (FSB). SORM-3 includes deep packet inspection competencies.Centralized control machine A machine for the centralized control of the general public telecommunications community is under development, controlled by way of the Centre of monitoring and managing of the public conversation Networks (TSMUSSOP).This new machine requires ISPs to install gadgets which can monitor, clear out, and, if needed, absolutely block site visitors' wireless, theoretically allowing the Russian internet section to be disconnected from the global network..

US Cyber Strategy

While The United States of America's countrywide Cyber strategy shapes its center framework shielding the yankee people, the homeland, and the way of life. This pillar emphasizes the safety of federal networks, crucial infrastructure, and preventing cybercrime.Selling American prosperity the second pillar specializes in safeguarding highbrow assets, the digital financial system, and making sure monetary resilience.preserving peace through strength The third pillar highlights lively measures and deterrence, marking a shift from passive defense to enforcing luxurious effects on adversaries .Advancing American influence. The fourth pillar ambitions to sell a cozy net version and a multilateral approach to exert global influence .Shift closer to deterrence The strategy explicitly commits to using all equipment of country wide power diplomatic, financial, intelligence, cyber, and kinetic military to prevent and reply to assaults (United States of America, 2018).

Russian Doctrines

The doctrine for ensuring information security and the doctrine for mitigating cyber attacks.Mainly focus on resilience and prevention .Russia employs two complementary doctrines: one for records safety (prevention resilience) and every other for mitigating cyber-attacks (detection/response). organizational individuals encompass the Federation Council, the nation Duma, the government, the security Council, and authorized statistics safety forces.The doctrine focuses on countrywide safety, chance reduction, constant effort to enhance information security control, collaboration among forces, and precautions in overseas statistics safety (consisting of placing ethical values and risk evaluation).

Russia's method to countrywide statistics security and its doctrine for mitigating cyber assaults.The doctrine pursuits for strategic deterrence in facts technology, securing defense force' records, forecasting threats, protecting allies' pastimes, and neutralizing impacts that undermine historical and patriotic traditions. A system is being developed to guard Russia's technological infrastructure from computer assaults.The gadget protects information resources and guarantees their functioning throughout incidents. Its operation relies on employee help, which includes focused staffing, improved training, and development of educational bases for employees.

Cyber Security Institutions of United States

The implementation of the 2018 country wide Cyber method is based on a mature atmosphere of federal corporations with awesome, complementary roles. **Department of homeland protection (DHS):** specified as the lead enterprise for securing federal civilian networks (.gov) and crucial infrastructure. The strategy mainly duties DHS to "further centralize control and oversight," empowering it to comfy corporation networks and direct defensive moves.

Branch of protection (DoD) & the Intelligence community (IC) undergo extraordinary responsibility for protective country wide security systems (e.g., mil), defense networks, and intelligence structures. Their function extends past defense to consist of undertaking intelligence evaluation and offensive and protective cyber operations .

The Department of Justice (DoJ) & the Federal Bureau of Research (FBI)serve as the primary regulation enforcement entities for combating cybercrime. Their mandate consists of investigating cyber incidents, prosecuting malicious actors, dismantling criminal infrastructure, and countering transnational cybercriminal businesses. **Workplace of control and budget (OMB):** Holds vital oversight and budgetary authority. OMB guarantees that cybersecurity chance control is aligned with IT budgeting , imposing compliance with policies and directives to pressure accountability.

National Institute of Requirements and generation (NIST): Operates as the primary developer of cybersecurity standards, frameworks, and quality practices. NIST leads tasks which include developing quantum resistant cryptographic algorithms, putting the technical foundation for security across authorities and industry (America, 2018, p. 8).

The method orchestrates a whole-of-government technique DHS centralizes civilian safety, DoD/IC consciousness on countrywide security and cyber operations, DoJ the law, OMB manages hazard through budgets, and NIST establishes the technical requirements.Centralization of DHS's function The branch of homeland security (DHS) is formally strengthened as the lead organization for protecting federal civilian networks and important infrastructure (America, 2018, p. 6).

supply chain safety is diagnosed as an awesome danger, the method requires integrating risk management into procurement and setting up a centralized evaluation service (u.s.a., 2018, p. 7).

Partnership with the private quarter: Emphasizes the want to encourage investments in security and collaborate with network operators to hit upon threats on the network stage.

protection of an open net: promoting an open internet version is framed as a countrywide safety precedence to counter authoritarian alternatives .

Russia Cyber Operation services

Russia special services involved in cyber operation service from **GRU or GU** main Directorate of the general staff of the armed forces provide services through groups of APT28 (Fancy Bear ,Pawn Storm Strontium and sofacy) ,Cyber Berkut, Sand Worm, Cyber Caliphate. These All groups Target the Ukraine (elections and critical infrastructure) 2014 ,Germany (Parliament) 2015,France media 2015,US elections 2016,midterm elections 2018,France elections 2017 ,Montenegro government 2016 to 2017,WADA/Sports organisation 2014 to 2018, OPCW 2018, Winter Olympic Games 2018,Georgia (Parliament ,media) 2019.(Kovacs, 2015).

Under the Federal security Service **FSB,** Turla APT (Snake, Uroburos, Waterbug, Venomous Bear) groups target Ukraine since 2014,35 countries (acting as Iranian hackers) 2019,US government 1990,Germany (Water and Energy companies)2020.

SVR Foreign Intelligence Service , APT29 (Cozy Bear, Office Monkeys, Duke, Cozy Duke, Cozycar) Groups targets the US (Elections ,NGOs ,Think tanks) 2016, Netherlands Government(2017),US (government ,military)2014-2015. Anti -COVID vaccine in UK, US, CAN 2020.(Haines,2014).

Internet and Legal Guidelines

Russian internet and media legal guidelines enacted between 2013 and 2019.

Prosecutorial net blockage regulation (398-FZ) gives authorities strength to block websites without a trial.(2013).

Numerous laws had been introduced, such as those penalizing "fake facts" about the **usa's** position in WWII (128-FZ), mandating records localization (242-FZ), requiring cellphone numbers for public access (no. 758), and proscribing overseas ownership of media companies to twenty% (305-FZ).(2014).

The 'Yarovaya' package deal of laws (374-FZ and 375-FZ) requires internet organizations to store content material (2016).

Legislation to modify messenger services (241-FZ) and outlaw VPNs (276-FZ).(2017)

The Sovereign net regulation (ninety-FZ) requires software installation to filter ,permitting Russia to disconnect from the global net in an emergency(2019).

Table 1
Comparative analysis United States vs.Russia:

Dimension	United states	Russia
Cyber warfare Doctrine	Cyber area is recognized as a proper war fighting area along land ,wind,ocean and area; Doctrine emphasises protection, deterrence and proactive engagement.	Russia has an information Warfare doctrine,integrating cyber electronic ,psychological and information equipment into a single operational idea.
Department Architecture	Department of Homeland security ,NSA, strong public private partnership ,department of Defence and US cyber command(USCYBERCOM)	GRU,FSB,General Staff of the Armed Forces and other limited civilian security services.
Cyber Policies	Governed through transparent coverage files, government directives and legislative oversight	Policies frameworks are opaque ,aligned with regimes, security centralized and priorities into

	;aligned with word wide norms and alliances commitment	world wide norms.
Strategies	National Cyber strategy Emphasize Shield ahead and persistent engagement aiming to disrupt Threads at their supply earlier than they attain us networks. Military Cyber Strategy cyber operations are incorporated with joint Kinetic operations under unified command structures and military making plans.	In Russia national cyber strategy specialized in non stop opposition under the edge of armed struggle , prioritizing strategic and ambiguity Military cyber strategy has cyber operations that coordinate with intelligence, create influence on campaigns and digital conflict in preference to conventional Army making plans alone.
Offensive and defensive cyber strategies	In offensive warfare Precisions targeted ,intelligence operations designed to degrade competencies and deterrence Emphasize essential infrastructure safety ,statistics sharing,resilience and speedy incident reaction.	Disruptive and Destabilizing operations emphasizing psychological, social effect ,political and technical precision. Defensive efforts priorities control of home records area and safety of Kingdom authority.

NATO doctrine considers cyberspace an operational domain in the facts surroundings, involving physical, digital, and cognitive dimensions. Western democracies awareness on preserving a unfastened, stable, and open internet, perceiving records security as the safety of information and systems, no longer controlling consumer ideals. The Western view of interstate war makes a clean distinction between struggle and peace primarily based on international law (UN charter).

Russia exploits the openness upheld in Western democracies to advantage records superiority, irrespective of a traditional war kingdom.Russia views its domestic information area as an extension of its territorial borders, subject to consistent overseas intrusion.

NATO considers our online world as an operational area inside a broader information surroundings that consists of physical, virtual, and cognitive dimensions.

opposite to the Western view, which distinguishes between war and peace based totally on international regulation, Russia perceives "records war of words" as steady and ongoing, permitting sports beneath the brink of armed war.

The Russian idea of "statistics guns" is huge, encompassing no longer simplest digital measures but additionally disinformation, electronic warfare, mental stress, and the degradation of navigation help.

A key Western aim is a unfastened and open net, in which facts safety means protecting facts and structures, not controlling beliefs.Russia seeks to take advantage of this Western openness to gain information superiority.records confrontation abilties and strategic objectives.

Conclusion

Cyber warfare has emerged as a great and complex mission within the realm of internet safety, representing a brand new geopolitical frontier that has basically reshaped how to understand and respond to threats .The United States has historically emphasized deterrence strategies, and the development of a criminal and coverage framework to govern cyberspace. While Russia prioritizes digital sovereugnity ,information disagreement and hybrid techniques that combine cyber operations with political and economic gear. It has highlighted the great interdependence of states on digital infrastructure and the corresponding dangers related with proliferation of cyber skills. The position of cyber

international relations, confidence-constructing measures, and collective defer initiatives can not be overstated in efforts to mitigate the security dilemma and prevent escalation of cyber conflicts.Russia's cybersecurity coverage, however, is most carefully connected with its traditional country wide safety pastimes and employs cyber guns as the issue a part of hybrid threats. Cyber protection as a device of record battle has become a detail of Russia's military method that allows you to reveal accelerated energy abilities and preserve a navy strain on fighters while warding off direct army struggle., America and Russia need to carefully apprehend the character of the brand new world with its relations to their own. protection and the safety of the arena, consequently making smart selections to provide safety even as selling cooperation. cybersecurity can be possible. If Russia and America can begin to open the doors of their cyber homes a little more extensively, this will be a chief step towards constructing trust, safeguarding information infrastructure, and selling an open records society at the worldwide stage.The future of cybersecurity will constructively depend upon how international locations are going to clear up. their competition issues while they realise that it additionally dictates the want for a more secure and extra secure.

Recommendations

Global cyber regulation,Russia and America need to undertake joint coverage assessments of jail additives of regulating cyber war offensive and defensive sports.

NATO-Russia cyber navy wearing events and exchanges.In the framework of NATO-Russia medical cooperation, Russia and the United States need to engage in reciprocal statement of and participation in simulations of cyber attacks.

Public Key Infrastructure Russia and the United States must champion in the global Telecommunication Union (ITU) the concept of a binding multilateral agreement on Public Key Infrastructure (PKI) to sell the world over an "atmosphere" depended on identities. Establish clean Cyber Doctrines Each state needs to articulate obvious cyber strategies that outline objectives, appropriate behavior, and escalation thresholds to lessen misperception and unintended war.

Workout Restraint in concentrated on Civilian Infrastructure restricting offensive cyber operations in opposition to vital civilian systems could beautify strategic stability and decrease humanitarian and monetary risks.

Toughen Cyber Resilience and defensive competencies cybersecurity frameworks, important infrastructure safety, and superior shielding technology is vital for national and monetary protection.

Have interaction in international Cyber Norm-constructing active participation in multilateral efforts to expand and implement norms of responsible kingdom conduct in our online world .

Lessen Escalatory facts and Hybrid struggle Practices Scaling lower back disinformation has an impact on operations.

References

Allen, G. C., & Chan, T. (2017). *Artificial intelligence and national security.* Belfer Center for Science and International Affairs, Harvard Kennedy School.

Binnendijk, A., (2020, June 2). Autonomous systems and the escalation of conflict. *RAND Corporation*

Centre for Strategic and International Studies (2025, June). *Significant cyber incidents since 2006.* Centre for Strategic and International Studies

CISA, (2021). Executive order on improving the Nation's Cybersecurity, CISA

Connell,M., & Volger, S. (2016). *Russia's approach to cyber warfare* (No. DOP2016U014231Final)

Foundation for Political, Economic and Social Research (FPRI), (2015). *Russia's use of disinformation in the Ukraine conflict.* Foundation for Political, Economic and Social Research (FPRI).

Haines, J. (2014). *Three NATO websites disrupted by Ukrainian hackers of Cyber Berkut*. Softpedia.

Hancock, B., Nguyen, H., Karpoyan, O.,Ear,E.,&Xu,S.(2025). Understanding Russia's Cyber Policies,Strategies,and Doctrine.*Military Cyber Affairs*, 8(1),11.

Khalid, U. (2025). The Digital Battlefield : A Comparative Analysis Of AI -Driven Cyber Warfare in the US and China and Its Implications for Pakistan's National Security. *ASSAJ,* 4 (01), 64-76.

Khan,Z.F.(2025).Cyber Warfare and International Security: A New Geopolitical Frontier. *The critical review of Social Sciences Studies*, 3(2),513-527.

Kovacs, E. (2015). *Cyber Berkut graduates from DDoS stunts to purveyor of cyber attack tools.* Recorder Future.

Kumar,S.,Benigni,M.,& Carley,K.M.(2016,September).The impact of US cyber policies on Cyber attacks trend. In *2016 IEEE conference on Intelligence and security Informatics (ISI)* (pp. 181-186*).*

Naftaliyev,S.(2025).Evaluating the United States National Cyber Strategy, *SSRN* 5590910.

Schaub, G., Jr., & Maurer, T. (2021). USCYBERCOM and the integration of artificial intelligence. *Survival*, 63(2), 123–144.

Shahbaz, K., & Muzaffar, M. (2025). The Russia-Ukraine Conflict and Its Implications for Regional Security: Assessing the Impact on Pakistan's Stability and Strategic Interests. *Pakistan Languages and Humanities Review*, *9*(2), 307–318.

U.S Department of State, (2018,March 26). *Statement from the Press Secretary on the expulsion of Russian intelligence officers*. U. S Department of State

Yaseen, Z., Muzaffar, M. & Aman, A. (2022). Russia-Ukraine War and Hybrid Attitude of European Union: A Critical Analysis, *Pakistan Journal of Social Issues, XIII,* 180-185