International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 7, Issue 7
July, 2024
Pages: 1-16

Militarization of Cyberspace and its Implications on National/International Security

Opeoluwa Adisa Oluyemi

Ph.D., Lecturer in the Department of Politics and International Relations, Near East University, Turkey

E-mail: opeoluyemio@gmail.com

http://dx.doi.org/10.47814/ijssrr.v7i7.2192

Abstract

The paramountcy of cyberspace together with the strikingness of globalization have transformed the universe into a global village, fostered businesses around the globe, connected people and enterprises and created immense opportunities for economic related activity, and communication. Consequently, an increasing number of processes are now reliant on the interconnectedness of digital infrastructure, which has resulted to the emerging cyber threats against individual, national, international, commercial and private security actors. Cyberattacks have changed the perception of states towards the cyberspace, necessitating the rising militarization of cyberspace by many countries leading to the advancement and development of their cyber military capabilities. This has created threatening conditions to the national/international security of states such as; the possibility of cyberattacks or cyberwar among states or non-state actors as well as the strategic leadership competition among powerful states such as; the U.S., China and Russia within the cyber domain. The militarization of cyberspace by these states and their perceptions of cyber threats from the advancement of cyber military capabilities of each state based on the realist thinking of international relations/security are formulated debates within this research. The research relies on secondary sources and employs a qualitative research approach, which reviews current literature on the topic under study to aver the potential transformation of the traditional/physical armed conflicts in the world into cyberwarfare as a result of the ongoing militarization of cyberspace constituting the fragility of national/international security.

Keywords: *Cyberspace; Cyberattack; Cyberwarfare; Militarization; International Security*

Introduction

The proliferation of Information and Communication Technologies (ICTs) has resulted to cyberspace becoming a major concern for states' policy-makers and of increasing interest to scholars of international relations or security studies. Ranging from financial losses to business enterprises through cybercrime to the theft of classified data of government and targeting of states' critical infrastructure, cyberspace has globally become a significant challenge to the economic and national security of states whereby it has been considered as the fifth domain of warfare after land, sea, air, and space (Craig & Valeriano, 2018). The impact of the information age on warfare has occupied the security concern for states' policy makers, soldiers, strategists, and non-state actors delving on the best ways of its utility and protection from potential threat of cyberattacks. This version of war is different from the traditional/physical war and not restricted to particular actors within the system, characterized with the capacity of attacking important systems in both states and non-states cyber domain, which could possibly cripple the entirety of societies that have become reliant on information technology (Greathouse, 2014). Some examples of cyberattacks experienced in the world over the years are; *"the 2007 cyberattack on Estonia, the 2008 attack on the state of Georgia, the Stuxnet virus from 2009 that attacked the Iranian nuclear program, and the actions by the hacker group "Anonymous" against companies such as; Visa, MasterCard, PayPal, and Amazon over the Wikileaks scandal"* (Greathouse, 2014, p.22). Noteworthily, each attack is an illustration of the potential destructiveness of cyberwar. According to Geers, (2011), the fact that cyberwarfare is an unconventional and asymmetric warfare has afforded weak nations lacking the capacity of conventional military power with the privilege of investing in cyber capability as a way of offsetting their conventional disadvantages.

The development and intensive use of advanced data processing technologies illustrating the popularization and massification of utilizing internet together with the influence of globalization has made cyberspace an environment embedded with several conflicts among states, political groups, criminal groups and companies. Undoubtedly, information or knowledge control has become a strategic asset for any organization, company or state (Rocha, 2019). This present dispensation has experienced an advanced utility of internet whereby virtually everything is connected to the internet and not only phones or computers but also critical infrastructure thereby, the world has now become increasingly interconnected through the cyberspace and internet. Cyberspace has created a global village, fostered business around the globe, connected people and enterprises and created immense opportunities for economic related activity, and communication. Consequently, an increasing number of processes are now reliant on the interconnectedness of digital infrastructure, which has resulted to the emerging threats against individual, national, international, commercial and private security actors (Kremer & Müller, 2014). This is illustrated in the statement released by the U.S. government Cyberspace Policy Review that; *"the architecture of the Nation's digital infrastructure, based largely upon the internet, is not secure or resilient. without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations"* (Kremer & Müller, 2014, p.43). As put forward by Cavelty (2008) that, states and enterprises are battling with these newly emerging threats as a result of the interconnectedness of digital infrastructures, threats that both government and private actors are unable to address. Foreign governments and non-state actors are infiltrating companies or state facility networks to steal and publish sensitive data or cause physical damages to critical infrastructure. The Canadian Government defined critical infrastructure as *"processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of the population, and the effective functioning of government. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence*" (Canada, 2009, p. 2).

The realization of these vulnerabilities embedded in cyberspace, most in particular those that potentially pose threatening conditions to the national defense of states has compelled many countries to embark on the use of their states armed forces to protect the cyberspace leading to the development of both offensive and defensive actions in this domain illustrating the basic tenets of militarization of cyberspace within the scope of this research. According to Cavelty (2008), several states have prioritized the use of armed forces within their defense attribution to ensure the protection of their countries not only against physical threats within the traditional attacks but also against those from cyberspace as a result of the prevailing various cyberattacks and virtual conflicts. Militarization is defined according to Schofield, (2007, p.11) *as "the measure of the extent of use of military structures and procedures in a state's decision-making process … the militarization of a state's decision-making process occurs when the military, or those possessing a military perspective, obtain relatively greater influence and the civilian policy-formulation institutions obtain relatively less influence."* A more elaborated definition of militarization was provided by Klare, (1978, p.121), as *"the tendency of a nation's military apparatus (which includes the armed forces and associated paramilitary, intelligence and bureaucratic agencies) to assume ever-increasing control over the lives and behavior of its citizens; and for military goals (preparation for war, acquisition of weaponry, development of military industries) and military values (centralization of authority, hierarchization, discipline and conformity, combativeness and xenophobia) increasingly to dominate national culture, education, the media, religion, politics and the economy at the expense of civilian institutions."* In addition, militarization of cyberspace is defined by Olszewski, (2016, p.104) as an *"increasing saturation of the state structure with ICT technologies and the growing importance of these components in the process of ensuring security"* According to Gomez, (2016, p.48), there are three main criteria of identifying the militarization of cyberspace by states; *"(1) A military doctrine or policy regarding cyberspace (2) A national cybersecurity strategy that recognizes state or state-sponsored cyber threats, and (3) A military and/or civilian unit(s) involved in to cyber defense and/or offense."* For the sake of this research, militarization of cyberspace is defined as a successful attempt of states to construct cyber domain as a major security threat to their national security legitimizing their adoption of military-oriented measures to address these emerging cyber threats, legitimizing their endless advancement/development of cyber military capabilities. The fact that, realist theory of international relations/security and its various strands have been widely employed by scholars to explain various military-oriented practices of states together with the contribution of this theoretical debates to the military events of the Cold War justifies its suitability as theoretical framework of this research aiming to applying the realist/neorealist postulations to the militarization of cyberspace and its potential implications on national/international security.

Conceptual Clarification

The first logical attempt of removing confusion from the study of cyber-related subjects is to define some popular terminologies associated with the study considering the fact that, many of these terms are used interchangeably. This research will thereby start by clarifying certain relevant terms through the analysis of existing definitions provided by the research community. Cyberspace or cyber domain is defined according to Segal (2016) as the *"the global network of interconnected information technologies and the information on it"*. According to Akdag (2018, p.3), cyberspace is defined as *"a global, political, and operational domain framed by use of electronics and the electromagnetic spectrum in order for the creation, storage, modification, exchange, and exploitation of information via interdependent and interconnected networks (and computer-based systems) using information communication technologies"* It has been considered as a new fifth military domain, along with air, land, space, and sea. Tabansky, (2011) argued that, cyberspace consists of a virtual environment that is composed of information, formed by computer networks that transmit it and connect computerized systems, through which information may travel, be stored, accessed and modified. Therefore, internet is considered as one of the main components of this environment, which is a global communication network that was created in 1980s and early 1990s (Cavelty; Mauer; Krishna-Hensel, 2007).

Cybernetics is defined as the potential threats and consequences associated with the intensive use of advanced technologies that support the transmission and processing of data of interest to institutions, companies, irregular or terrorist groups, and states (Rocha, 2019). Cyber issue has to do with potential negative outcomes that cyber threats may have, mainly, on national state' security and defense or non-state actors (Rocha, 2019, p.522). In addition, they are also emanating issues from lack of control and widespread use of cyberspace such as; acts of espionage, sabotage, and attack/war, possible through cyberspace. Cyberattack is defined as "*deliberate actions to alter, disrupt, deceive, degrade, or destroy computers or information networks and/or programs that reside or transit through these systems or networks”* (Caplan, 2013, p. 2). According to the U.S. Army Training & Doctrine Command (2006), cyber-attack is defined as *“the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.”* Cyberattack is also defined according to Lin (2010, p. 63) as *"the deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or training these systems or networks.”* Cyber espionage is different from cyberattack as it involves the penetration into the adversary’s computers or networks through a worm or malware to monitor and obtain information for intelligence purposes (Bajaj 2010, p. 2). In addition, contrary to cyberattack, it does not cause critical damage to data or network but the information processed from cyber espionage can be instrumental for the destructive activity relevant as cyber weapons in a cyberattack. Cyberwarfare involves *"the confrontation of one or more states, as well as diverse political or criminal groups, and is based on exploiting security breaches in this environment to harm the potential adversary"* (Rocha, 2019, p.523). The need to examine this new type of war has attracted the attention of many scholars with the argument that, unlike nuclear explosion resulting to death of millions, the possible disruption from cyberwarfare could generate the same outcome (Rocha, 2019). As put forward by Cetron & Davies (2009, p. 47) that, “*major concern is no longer weapons of mass destruction, but weapons of mass disruption”* This information warfare is defined according to Rhona (1976) as *“the strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives”* (cited by Libicki, 1995). The Shanghai Cooperation Organization has defined this information war as a *“confrontation between two or more states in the information space aimed at… undermining political, economic, and social systems [or] mass psychologic brainwashing to destabilize society and state”* (Gjelten 2010, p. 36). Another significant attribute of this emerging global (virtual) conflict is the possibility of non-state actors engaging in cyberwarfare (Klimburg, 2011). According to Nye (2010, p. 6*), "the actions of “hacktivists” including the group Anonymous or “patriotic hackers” and actions taken during the 2007 cyber*-attack *on Estonia or the actions of Chinese or Taiwanese hackers are all indicative cases of non-state actors engaging in this form of conflict"* The broadening of actors who are participants of this conflict is as result of the growing use of information and technology across the globe. As put forward by Alford (2001) that, the growing use of information facilitates an increasing threats to the control of civilization. Cyber weapons include viruses, malware, denial of service, spying, along with jamming and blocking (Saad et al. 2011, p. 4). Lastly, cybersecurity is defined according to the International Telecommunications Union (ITU) as *“the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets”* (ITU, 2009).

Theoretical Framework

Realism and Cyberspace

Realism is mainly classified into two; classical realism (Thomas Hobbes, Thucydides and Niccolò Machiavelli) and neorealism (Kenneth Waltz and Mearsheimer). The other unpopular branch of realism heavily criticized by realist scholars is known as neo-classical realism (Gideon Rose, Norrin M. Ripsman, Jeffrey W. Taliaferro, Steven E. Lobell, and Fareed Zakaria). Classical realists focus on human nature as the primary reason for competition, origin of war, importance of power and international conflicts. Thucydides for example argued that, the divergent ambitions of state are drivers of international conflict rooted in the human capacities for pride and fear. Structural realism argued that international system is the source of competition among states, balance of power and the need to pursue power for the survival of states. The international system creates incentives for all great powers regardless of their regime types, domestic institutions and culture. Furthermore, the two key strands of neorealism are; offensive and defensive. Defensive neorealists such as; Kenneth Waltz (1979) argued that, it is erroneous and unnecessary for states to endlessly pursue power due to the possibility of a backlash for wanting too much of it thereby, the maximization of sharing world power is deemed a foolhardy one. While offensive neorealist argued contrary to this stating that, it is necessary and prudent for states to pursue more power as much as possible and under the right circumstances to pursue hegemony (Mearsheimer, 2001). The accumulation of overwhelming power is a prudent mean of ensuring the survival of states within international system. The emerging branch of realism that contradicted the basic attributed features of realism (self-help, state-centric and survival) is neo-classical realism, which presented a theory of foreign policy recognizing the domestic politics and non-state actors' involvement in national and international politics (Ndzendze & Marwala, 2023). Realism has been considered as suitable theoretical framework for analyzing the militarization of cyberspace by some scholars. According to Reardon & Choucri (2012, p.6), *"realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilizing or destabilizing, whether cyber technologies will be a new source of conflict or of peace, and whether states will engage in cyber arms racing."*

Cyber-conflict is explained to have originated from the development of concepts of ‘cyberwar’ and ‘net-war’ by Arquilla & Ronfeldt (1993) with the prediction of a possible transformation of warfare in line with rapid advances in ICT. It is defined according to Valeriano and Maness (2015, p.32) as "*the use of computational technologies in cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities."* The fact that, cyber-threats have been constructed today as a top priority of national security concern whereby governments of states are paying adequate attention to all possible cyberattacks against their vulnerable critical infrastructure from both states and non-state actors resulted to the realist/military-oriented approaches employed to address it. The U.S. Defense Secretary in 2012 for instance, issued a warning concerning a cyber ‘Pearl Harbor’ against the power grid or the financial system in which both are dependent on computer networks for their operation (Bumiller & Shanker 2012). In addition, a conducted survey in 2016 showed 27 percent of Americans agreed that cyber-terrorism posed a serious threat to the United States (Bumiller & Shanker, 2012). In order to analyze the contribution of realism to these emerging cyber issues, certain established realist postulations are found applicable to the present cyber-related issues. The first consideration is the concept of anarchy in realism and its application to cyberspace. Anarchy is the fundamental assumption underlying structural realist theories referring to the absence of overarching authority to police the international system, which compels states to rely on self-help measures in order to achieve security or pursue their national interests (Waltz, 1979). In an anarchic environment, where states seek to satisfy their own interests, there is a constant possibility of war (Waltz, 2001). Realism argues basically on the inevitability of war among states since there is no entity or centralized authority capable of preventing interstate armed confrontations (Waltz, 2001). Baylis & Wirtz (2002, p.7) argued that, *"in the absence of world government, realists note that states have adopted a ‘self-help’ approach to their interests and especially their security. In other words, they reserve the right to use lethal force to achieve their objectives."* This realist anarchical nature of international system is applicable to the absence of international law or institution regulating or governing the cyberspace raising the question of how to define the end to the war in cyber domain with no laws governing virtual conflict and no limits to set a demarcation line of attack and defense? Based on the Sanremo Handbook on Rules of Engagement, prepared under the guidance of the International Institute of Humanitarian Law, the distinctive feature of cyberspace is stated as a notional environment beyond the jurisdiction of any single nation, which means the possibility of war in this space is endless, limitless and disorientating (Cole etal., 2009). As put forward by Lancelot (2020, p.3), that, *"the problem, therefore, is cyberspace has extended* *the anarchic component of the Westphalian international state system into a virtual and lawless territory, undermining the current world order"*

The concept of cyber-power is another area of existence of similarity between the characteristics attributed by the realists to the international system and characteristics embedded in cyberspace. Power is one of the basic tenets of realism because it can grant the independence and survival of the state in a self-help environment (Mearsheimer 2006, 79–81). As put forward by Morgenthau (1948, p.13) that, *"whatever is the ultimate aim of international politics, power is always the immediate aim."* Power is basically considered as the main asset of state like natural resources, industrial capacity, military strength, and population a state possesses (Morgenthau 1948, p.80). The distribution of power among states has implications for stability within international system, it is how states are classified within a multipolar, bipolar, or unipolar power configuration (Mearsheimer, 2006). Cyber power on the other hand is defined according to Nye (2011, p.3) as *"the ability of a state to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain",* and its potential implication of transforming international relations/security has occupied different debates within the discipline. Noteworthily, there is no theory of cyber power expounded within the realist thinking of international relations in which the central argument of realism describing states as the most powerful and significant actor of international politics is now questionable considering the notable involvement of non-state actors threatening the traditional power dynamics of states in this era of information revolution (Eriksson & Giacomello, 2006). However, Nye's (1990, p.160) argued on the theory of power diffusion, which is applicable to cyber domain whereby individual criminals, organizations, and terrorist groups with the privilege of access to internet are able to threaten the dominance of states and private enterprises, playing significant role as providers of security and as sources of vulnerability (Craig & Valeriano, 2018). Another reality of cyber power interesting to realism is the fact that, as a result of the relative low cost of entry into the cyberwarfare domain, weak states with traditional military incapability are now able to challenge stronger states leading to power reconfiguration within the power distribution system (Lango, 2016). The training of thousands of hackers by North Korea (Mulrine 2016), the accusation against the China's Unit 61398 of committing cyber espionage campaigns against the United States (Mandiant, 2013), and the increasing sophistication in cyberwarfare tactics of Iran (Aitel, 2015) are exemplifying cases of this reality. Traditional power dynamics has been undermined through cyber-power with the paradoxical idea that, the most technologically advanced countries are also the most dependent on digital infrastructure and thus the most vulnerable to a crippling cyber-attack (Kolet 2001, p.282). Lindsay (2013) on the other hand, has argued that the only technological advantage under the possession of superpowers are their abilities to develop powerful sophisticated cyber weaponry, which has depicted the asymmetric nature of cyber domain.

Another prominent area of realism applicable to the ongoing preponderance of cyber conflict among states and non-actors in this dispensation is the offense-defence balance of power theory that constituted the different strands of neo-realism. The idea that attacking is cheaper, easier, more effective, less demanding than defending that characterizes security strategy in the cyber security discourse has demonstrated cyberattacks to be more in line with offensive realism (Lieber, 2014). Mearsheimer (offensive realist) departs from Waltz (defensive realist) in his assertion that the search for power and security is insatiable, whereas Waltz argues that it has limits. *"For defensive realists, the international structure provides states with little incentive to seek additional increments of power; instead it pushes them to maintain the existing balance of power. Preserving power, rather than increasing it, is the main goal of states. Offensive realists, on the other hand, believe that status quo powers are rarely found in world politics, because the international system creates powerful incentives for states to look for opportunities to gain power at the expense of rivals, and to take advantage of those situations when the benefits outweigh the costs. A state's ultimate goal is to be the hegemon in the system"* (Snyder, 2002, p.152). Offensive realism according to Mearsheimer has suggested the possibility of more conflicts and war among states than defensive realism of Waltz whereby Mearsheimer deduces that great powers will fear each other and will constantly seek to alleviate this fear by maximizing their share of world power (Snyder, 2002). Technological factors are explained within the debates of offense-defence balance in different ways whereby mobility enhancing technologies are considered to be in favour of attackers, whereas technologies that increase firepower make defending more effective (Glaser & Kaufmann, 1998). According to Lieber (2014, p.100), cyber offense is considered more effective than defence due to its cheapness and ease, the ability to cause critical damages to the society, its instantaneous nature and attack only needs the vulnerabilities of the target to succeed whereas defence is more demanding as it must ensure the safety of entire networks and continuous patching of vulnerabilities that the defender is unaware of before they are exploited for potential attack. This explains the potential eruption of virtual conflict in the world and the fragility of national/international security when offensive action is considered more advantageous and easier than defensive capabilities. This also justifies the concept of arms-race within realist theory whereby the advancement in military capability of one state is a potential security threat to another state for possible attacks thereby, states are in constant competition to augment their military capabilities for the sake survival. The various approaches adopted to militarize cyberspace by powerful states such as; the U.S., Russia and China or rising states like Iran, Israel and India leading to their endless development and advancement in cyber military capabilities are illustration of the realist postulation of arms-race, which has become threatening to the stability of international security.

Militarization of Cyberspace and Fragility of International Security

Cyberwar is described as non-kinetic capable of causing physical damage to cyber infrastructure (Firdous, 2020). Every operation of cyber capability that is non-kinetic is regarded to as Computer Network Operations (CNO) according to the United States Army. CNO is further divided into three namely; Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA) (Spade, 2011). CNE is naturally intrusive and generally non-destructive such as cyber espionage while CNA can be notably destructive, which are offensive cyber operations that can potentially cause psychical damage such as; cyberwar or cyberattack (Spade, 2011). Cyberattack is further differentiated from cyberwar according to Ben-Israel & Tabansky (2014) with the argument that, in order to consider a cyberattack as an act of war, the following conditions must be put into consideration; "(a) the organizational and geographical sources: the finding of whether a state is behind the action (b) motive: the possibility of identifying an ideological, political, economic, or religious motive behind the attack (c) level of complexity: the level of complex planning and coordinated resources that are exploited primarily by state agencies (d) results: the criticality of the damage associated with the attack and casualties, and the level of damage it could cause without proper defensive actions" (Ben-Israel & Tabansky, 2014, p.59-60). The recognition of cyber domain as an operational realm for potential attacks against the national security of states resulted to the need of incorporating cyber defense/offense into their existing military structures. Countries such as; the U.S. and North Atlantic Treaty Organization (NATO), China, Russia, Britain, Germany, France, Israel, and India started to develop different cyber policies and strategies such as; the establishment of cyber mission force, cyber units, cyber commands, and cyberattacks as means of cyber defence and many other countries have started the process of incorporating these components into their armed forces (Firdous, 2020). According to Hughes, (2010), the last two decades have witnessed different cyber operations such as; espionage, sabotage, and subversion against their oppositions. These are exemplified as *"Chinese cyber-attacks on several secure systems of the US government offices such as; the Department of Defense (DoD), Department of State, Department of Homeland Security (DHS), National Aeronautics and Space Administration (NASA), and the Office of Foreign Commonwealth in the UK, 2007 cyber-attacks against Estonia and 2008 computer network operations on Georgia, and more significant and coordinated cyber operation on Iran's nuclear facility, Stuxnet"* (Firdous 2020, p.81).

The United States has been described as the home country to cyber technology and the first country to divert cyberspace to national security concern (Ameli, Hosseini & Noori, 2021). At the immediate aftermath of 9/11 attacks, the U.S. cyber strategy focused on enhancing federal computers and IT infrastructures security as demonstrated in the executive order of George Bush in October 2001 *"authorizing a protection program that consists of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems"* (The National Strategy to Secure Cyberspace, 2003, p.14). The then president also requested for the increase of funds from the Congress in year 2002 to ensure the security of federal computers by 64 percent for the fiscal year 2003. The militarization of cyberspace by the United States was formalized through the formation of "*the National Military Strategy for Cyberspace Operations*", released by the Joint Chief of Staff in 2006. This official document emphasizes on the significant role of the U.S. Armed Forces to ensure the superiority of the U.S. in cyberspace by conducting different military operations. This strategy stated that, the U.S. has started *"the integration of cyberspace operations with DOD's national defense role in the areas of military, intelligence, and business operations in the areas of military, intelligence, and business operations"* (The National Military Strategy for Cyberspace Operations, 2006, p.1). Cyberspace became officially recognized as a foundation for Command and Control (C2) of military operations in other domains in need of unified action vertically and horizontally among all levels of war (The National Military Strategy for Cyberspace Operations 2006, p.11). This was followed by the 2007 Comprehensive National Cybersecurity Initiative (CNCI) that engaged in different militarization approaches through the linking of the formerly separated cyber defensive missions with law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities (CNCI, 2007). The association of cyberattack with terrorism leading to cyber terrorism resulted to an increasing perception of cyberspace as potential security threats to the U.S. national security. According to the NSS (2010), *"cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy."* In another statement of the NSS argued that *"the threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states"* (NSS, 2010: 27).

Based on the realist thinking of cyber politics, the militarization of cyberspace by other states such as; China and Russia leading to the development in their cyber military capabilities are considered threatening to the United States national/international security. As stated by Dmitri Alperovitch, former McAffee cyber threat researcher in 2012*, "I can tell you that the Chinese have an aggressive goal to infiltrate all levels of U.S. government and private sector networks" China became threatening to the U.S. national security in cyberspace as result of the Chinese "cyber jedis"* (Hopkins, 2012). The military units assigned to carry out computer network operations (CNO) in China is the PLA's Third and Fourth Departments of the General Staff Department. The Third Department was established during the 1980s and the Fourth Department during the early 1990s. The Third Department is China's central signals intelligence organization assigned with two main duties; computer network defense (CND) and computer network exploitation (CNE) and the Fourth Department is legalized to carry out computer network attacks (CNA) as the electronic countermeasures organization (Firdous, 2020, p.83). Based on the report by the US-China Economic and Security Review Commission in 2012, it was stated that *"the Chinese People's Liberation Army (PLA) has long considered the ability to seize information dominance as prerequisite for achieving victory in future high tech conflicts, but only recently has it begun to develop the capability to convert this strategic requirement into an operational possibility"* (Krekel et al, 2012, p.14). Another report submitted to the Congress by the US-China Economic and Security Review Commission in 2012 suggested that China has been taking *"a multipronged approach to the cyber domain" with "numerous stakeholders [who] influence cyber-related activities and priorities and a broad, national-level enterprise of government and military"* (US-China Economic & Security Review Commission, 2012, p.147) and that Chinese hackers, including state-sponsored actors, continue to *"exploit U.S. information systems across government, industry, and civil society"* (US-China Economic & Security Review Commission, 2012, p.153). According to Krekel et al, (2012, p.8), China is alleged of trying to integrate CNO1 with other types of information warfare such as; electronic warfare, psychological operations, kinetic strike, and deception, and utilize them in a unified framework known as “information confrontation.” In addition, the availability of around 538 million internet users in China was allegedly described as China developing “a pool of cyber soldiers” (US-China Economic & Security Review Commission, 2012: 149-152) cited by (Ameli, Hosseini & Noori, 2021). According to Manson, (2011), there different ways at which China's offensive cyber capabilities can be evaluated; one of the ways is described as China's ability to place logic bomb known as malicious code in other nations’ networks. It is speculated that, China placed logic bombs in the U.S. computer-oriented systems, such as those of power grids and financial systems, which exemplifies this China's capability. Another China's offensive cyber capability pointed to its recruitment of civilian hacker groups as stated by Manson, (2011) that, the U.S.-China Economic and Security Review Commission in 2010 estimated around 250 patriotic hacker groups capable of conducting a variety of cyberattacks, ranging from unsophisticated denial-of-service attacks to perplexing cyber espionage and over 15.000 of these hackers are informally linked with Chinese government (Manson, 2011). The third way of ascertaining China’s cyber offensive warfare capability is described by Manson (2011) as the formation and training of cyber-units in its military sector.

Furthermore, the advancement in the cyber military capability of Russia is also considered threatening to the national/international security of the United States. Russia has historically demonstrated the tendency of engaging in cyberattacks through its attack against Georgia’s communications network in 2008 and the 2007 DDoS attack against Estonia (Ameli, Hosseini & Noori, 2021). Russia is allegedly suspected for the Denial of Service attack against Estonia, which literally wiped-out the country from internet (Tofan et al, 2012) because the attack happened when there was disagreement between the two states concerning the Estonian government’s removal of a Soviet war memorial from Tallinn (Thomas, 2009). It was suspected that some group of “patriotic hackers” in Russia got offended with this decision of Estonian government, which consequently resulted to the conduct of the cyberattack that was allegedly supported by the Russian government (Nye, 2010). In addition, the first experience of using internet during a conventional armed conflict to disrupt civilian use of the internet happened in the 2008 conflict over the Georgian province of South Ossetia. Georgia is said to have triggered the conflict as a result of attacking Russian soldiers assigned for a peacekeeping contingent in South Ossetia under the terms of a Georgia–Russia treaty of 1991, which resulted to the death of around dozen of Russian soldiers and left many wounded. Russia initiated a counter-attack of DDoS attacks against a number of Georgian websites, including government sites, media sites and commercial sites, which was followed by a physical military attack against Georgia (Connell, 2012). The U.S. ambassador to Russia, David Smith, stated that *“Russia has integrated cyber operations into its military doctrine”; though “not fully successful … Russia’s 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine … [and] we must assume that the Russian military has studies the lessons learned"* (Smith, 2012) cited by (Ameli, Hosseini & Noori, 2021, p.114-115).

Another area of militarization of cyberspace by the U.S. is described as the institutionalization of cyber military structures (Ameli, Hosseini & Noori, 2021). A coordinated military response to the possible cyberattacks by the U.S. started in 1998 with the formation of A Joint Task Force on Computer Network Defense (JTF-CND) under PDD-63. JTF-CND assigned with the role of protecting computer networks and systems of the DoD. In year 2003, the DoD shifted attention to offensive missions alongside with defensive operations in cyber domain. Considering the fact that, JTF-CNO has been unable to perform both offensive and defensive operations effectively resulted to the assignment of offensive operations to the National Security Agency (NSA) under the U.S. Strategic Command initially but a new component, known as Joint Functional Component Command Network Warfare (JFCC-NW) was created in 2004 under the U.S. Strategic Command to mainly carry out offensive operations. In 2009, the U.S. Cyber Command (USCYBERCOM) was formed and assigned with duties; "*to direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations to enable actions in all domains,* *ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries"* (Firdous, 2020, p.84). The operational roles and responsibilities of DoD in cybersecurity are conducted through USCYBERCOM Joint Operations Center, the National Security Agency/Central Security Service Center, the Defense Cyber Crime Center, and the Defense Information Systems Agency (DISA) (Pernik et al, 2016, p.20). As put forward by Deibert, (2011, p.2) that, the most notable approach towards militarization of cyber space adopted by the U.S. is the formation of the U.S. Cyber Command (USCYBERCOM) which unifies all of the existing military cyber activities under a single command. The cyber components of all military services are to report and provide support to USCYBERCOM such as; Army Cyber Command (2nd Army ARCY), Air Force Cyber Command (24th Air Force AFCY), Navy Fleet Cyber Command (10th Fleet FLTCY), and Marine Corps Forces Cyberspace Command (MAR4CY) (Firdous, 2020, p.84). In addition, during the second term of Obama administration, the DoD developed a Cyber Mission Force (CMF). CMF is described according to Pomerleau (2017) to consist of 133 teams and 6,200 personnel including *"13 National Mission Teams that defend the nation; 68 cyber protection teams that work to defend DoD networks; 27 combat mission teams that provide support to combatant commanders and generate effects in support of operational plans and contingencies, and; 25 support teams that provide analytic and planning support to the national mission teams".* Out of 133 CMF teams, the Army provides 41, the Navy provides 40, the Air Force provides 39 and the Marine Corps provides 13 (Pomerleau, 2017) cited by (Ameli, Hosseini & Noori, 2021, p.125).

Another militarization of cyberspace by the U.S. is described as the deployment of Stuxnet, which marked a revolution in the history of military operation. As put forward by Farwell & Rohozinski, (2012) that, Stuxnet attack represents a new era that is embedded with both implications and lessons pointing to the fact that *"cyberattack is not a distant theoretical probability" and that "cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary*. The attack took place in 2010 when it was launched to destroy 1,000 out of 9,000 centrifuges at the Iranian Natanz facility (Albright et al. 2011). Iran and its uranium-enrichment plant at Natanz was the target and based on the report of Microsoft, the attack affected around 45,000 computers whereby 60% of the infected machines, as Symentac a computer firm found in Iran, 18 % in Indonesia and 8 % in India (Clayton, 2010). According to Beaumont (2010), the main target of Stuxnet was SCADA system manufactured by Siemens that is widely used by Iran for different infrastructures. Considering the stated features differentiating cyberattack from cyberwar according to Ben-Israel & Tabansky (2014), Stuxnet has been considered as the only cyberattack that completely reflected an act of war, a computer virus developed by state that incurred physical damage against an adversary (another state) (Ameli, Hosseini & Noori, 2021). It was reported in the New York Times that, a special Israeli unit collaborated with the U.S. to launch cyberattack on Iranian enrichment facility (Sanger, 2012). This level of development of cyberspace for military operation has been described threatening to international security although, both countries have not confirmed their involvements or collaborations toward such operation. As a result, the Chinese government declared that, *"the U.S. military is hastening to seize the commanding military heights on the Internet"* (Reisinger, 2012). Additionally, there are progressively other worms beside Stuxnet since 2010 that have been used to launch attacks on different systems across the Middle East such as; *Duqu, Flame, Gauss, and miniFlame*. Eugene Kaspersky is a computer expert at the cybersecurity firm Kaspersky Labs commented that, the newly emerging cyber weapons have been a shock to everyone as nobody expects to find such a serious, very professional, huge project capable of constituting the fragility of international security (Firdous, 2020).

Discussion and Conclusion

Cyberspace has been described as a strategic security environment by states generally in the world however, the U.S. has attracted the attention of this research due to its leading role in the cyber world. According to NSS (2010, p.27), *"cybersecurity threats have become one of the most threatening* *challenges to the U.S. national security, public safety, and economic challenges. The very technologies that empower us to lead and create also empower those who would disrupt and destroy."* The National Military Strategy of the U.S. stated that, cyberspace has become a war-fighting domain thereby, the United States "*will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving the US's ability to attribute and defeat attacks on systems or supporting infrastructure"* (The National Military Strategy of the United States of America, 2011, p.8). The perception of the military nature of cyberspace coupled with the primacy to be dominant in this domain have occupied the national security agenda of the United States followed by China and Russia, describable as a depiction of military strategic competitions of powerful states (the U.S. and Soviet Union) during the Cold War. The fact that, realism/neorealism was the main theoretical explanation provided for the military events of the Cold War and the military oriented postulations of the theory justify its suitable applicability to analyzing the potential future eruption of cyber conflicts threatening the stability of international security. Noteworthily, many advocates of realist thinking have only focused on the potential impact that war technologies could have on war-related activities and explanation of factors that could lead to war among states. Therefore, technologies related to the internet and cyberspace as a whole were generally overlooked by these realist scholars disputing the possibility of states gaining or using certain military power through cyberspace (Rocha, 2019). However, despite the realists' restriction on cybernetics, it is arguably impossible to undermine the applicability of the basic tenets of realism and its various strands to the theoretical understanding of the ongoing militarization of cyberspace and its potential implications on international security.

In summary, there are five notable assumptions of realist/neorealist theory of international relations/security considerably applicable to analyzing the militarization of cyberspace and its possible implications on national/international security according to this research. Firstly; the realist assumption that international system is played out in an anarchical realm, which means there is no leadership or central government or authority to manage and regulate the excessiveness of states is considered applicable to the absence of international law or authority or body to regulate the cyberspace, which has created an enabling environment for limitless of cyberwarfare or cyber-attacks among states or from non-states actors. Additionally, the possibility of non-state actors launching cyberattacks against states, the cyber advantage of weak states with traditional/physical military incapability to attack powerful states, the problem of attribution inherent with cyberattacks, and the emerging multipolar balance of power configuration as result of the rising states in cyber military capabilities pose potential threatening conditions to the stability of national/international security of states. Secondly, the realist assumption that states cannot be absolutely sure of each other's intentions and uncertainty of states that other states will not use force against them. This realist thinking that, states suffer from imperfect information about each other's intentions explains the reasons why the U.S. would consider the advancement of cyber military capabilities of Russia, China and Iran or global south as potential threats. This consequently resulted to another realist concept of arms-race in cyberization of states in which there are strategic competitions among states (the U.S., China and Russia) to develop their military capabilities in cyber domain as a way of ensuring their survival, building their offense/defence cyber capabilities in order to exert power within the international system. This is found explanatory to the third realist assumption that, the primary motivations of all states within the international system are self-help and survival, which are basically attainable through the accumulation of military power and its endless pursuit.

Furthermore, the fourth realist assumption applicable to analyzing the militarization of cyberspace stated that, states are rational entities that think strategically about their external relations and also states strive to possess military power in order to exert influence and command/control within international system. This theoretically justify the desire of the U.S. for power accumulation to dominate in all areas including cyber domain as reflected in the Obama administration in both 2010 and 2015 that added the fourth basic principles of the U.S. constitution as; *"an international order advanced by U.S. leadership that promotes peace, security, and opportunity through stronger cooperation to meet global* *challenges"* (NSS, 2010, p.7). The desire for the leading role of the United States was also found in Hillary Clinton's remarks on the 2010 NSS, expressed on 27 May 2010; *"Our approach is to build the diverse sources of American power at home and to shape the global system so that it is more conducive to meeting our overriding objectives: security, prosperity, the explanation and spread of our values, and a just and sustainable international order"*. The NSS in 2015, also emphasized that: *"a strong consensus endures across our political spectrum that the question is not whether America will lead, but how we will lead into the future"* (NSS, 2015, p.2). This constitutes the fundamental of American approach to its various policies at national and international environment, which has been confronted with reactionary responses from rising states in the world facilitating the existing strategic competitions and instabilities of international security. The fifth and final realist assumption employed by this research to analyze the implications of militarization of cyberspace on international security is the positions of different strands within the realist theory such as; the neorealist defensive and offensive military attacks and neo-classical realism. The offensive realist debate has mainly rationalized the historical experience of cyberattacks and also a justification or rationale for a potential fast approaching military warfare that is transformative of traditional military attacks, suggested to be cyberwarfare among the powerful, weak and rising states as well as non-state actors with growing cyber military capabilities constituting the fragility of international security. The involvement of non-states actors in the militarization of cyberspace and as potential perpetrators of cyberattacks are outside the basic tenets of realist/neorealist arguments (statism: states are the primary actors of international system) however, the recognition of neo-classical realism by this research is an attempt to cover this theoretical gap.

References

Aitel, D. (2015). Iran is emerging as one of the most Dangerous Cyber-Threats to the US. Business Insider UK, 2 December. Retrieved from: http://uk.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyberthreats-to-the-us-2015-12?r=US&IR=T Accessed on April 22, 2024.

Akdag, Y. (2018). The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective. *Journal of Chinese Political Science/Association of Chinese Political Studies*, 4-23 https://doi.org/10.1007/s11366-018-9565-4.

Albright, D., Brannan, P., & Walrond, C. (2011). Stuxnet Malware and Nntanz: Update of ISIS December 22, 2010 Report. Institute for Science and International Security. Retrieved from:http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf Accessed on April 22, 2024.

Alford, L.D. (2001). Cyber Warfare: A New Doctrine and Taxonomy. Crosstalk*: Journal of Defense Software Engineering*, Vol. 14(4), 27–30.

Ameli, S.R. Hosseini, H. & Noori, F. (2021). Militarization of Cyberspace, Changing Aspects of War in the 21st Century: The Case of Stuxnet against Iran. *Iranian Review of Foreign Affairs*, Vol. 10 (1), 99-136.

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is Coming *Comparative Strategy* Vol. 12(2): 141–165.

Bajaj, K. (2010). The Cybersecurity Agenda: Mobilizing for International Action. East-West Institute Report. Retrieved from http://www.ewi.info/system/files/Bajaj_Web.pdf Accessed on April 30, 2024.

Baylis, J. & Wirtz, J. (2002). Introduction. In: Baylis, John; et al. Strategy in the Contemporary World: An Introduction to Strategic Studies. Oxford: Oxford University Press.

Beaumont, P. (2010). Stuxnet Worm Heralds New Era of Global Cyberwar. The Guardian. Retrieved from http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar Accessed on April 27, 2024.

Ben-Israel, I. & Tabansky, L. (2014). An Interdisciplinary Look at Security Challenges in the Information Age. In Siboni, G. (Ed.). Cyberspace and National Security Selected Articles II, 51-67. Tel Aviv: INSS Institute for National Security Studies.

Bumiller, E. & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S. The New York Times, Retrieved from: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html Accessed on April 22, 2024.

Caplan, N. (2013). Cyber War: The Challenge to National Security. *Global Security Studies*, v. 4, n. 1, p. 93-115, 2013.

Cavelty, M.D., Mauer, V., Krishna-Hensel, S.F. (2007). Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. 1. ed. Hampshire: Ashgate Publishing, 2007.

Cetron, M.J. & Davies,O. (2009).Ten Critical Trends for Cyber Security. *The Futurist*, Vol. 43(5), 40–49.

Clayton, M. (2010). Stuxnet Malware is ‘Weapon’ Out to Destroy. Iran’s Bushehr Nuclear Plant? The Christian Science Monitor. Retrieved from: http://www.colorado.edu/physics/phys3000/phys3000_fa10/articles-f10/0606.pdf Accessed on April 25, 2024.

Cole, A., Drew, P. & McLaughlin, R. (2009). Sanremo Handbook of Rules of Engagement. *International Institute of Humanitarian Law*, Sanremo, Italy; 2009. p. 1–86.

Connell, M.E.O. (2012). Cyber Security without Cyber War. *Journal of Conflict & Security Law*, Vol. 17(2), 187–209.

Craig, A.J.S. & Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. In D. Orsi; J.R Avgustin & M. Nurnus (Eds). Realism in Practice: An Appraisal. E-International Relations Publishing.

Deibert, R. (2011). Tracking the Emerging Arms Race in Cyberspace. Interview interviewer: Bass. Bulletin of the Atomic Scientists, Vol.67(1), 1–8. Retrieved from: http://journals.sagepub.com/doi/pdf/10.1177/0096340210393703 Accessed on April 26, 2024.

Eriksson, J. & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review* Vol. 27(3): 221–244.

Farwell, J. P. and Rohozinski, R. (2012). The New Reality of Cyber War. *Survival*, Vol. 54(4), 107-120. https://doi.org/10.1080/00396338.2012.709391.

Firdous, A. (2020). Cyber Warfare and Global Power Politics. *Center for International Strategic Studies (CISS)*, Vol. VIII(1), 71-85.

Gjelten, T. (2010). Shadow wars: Debating Cyber Disarmament. *World Affairs*, 173(4), 33–42.

Glaser, C.L. & Kaufmann, C. (1998). What is the Offense-Defense Balance and Can we Measure it? *International Security*, 22(4): 44–82.

Hopkins, N. (2012). Militarization of Cyberspace: How the Global Power Struggle Moved Online. The Guardian. Retrieved from: https://www.theguardian.com/ technology/2012/apr/16/militarisation-of-cyberspace-power-struggle Accessed on April 22, 2024.

Hughes, R. (2010). A Treaty for Cyberspace. *International Affairs*, Vol. 86(2):523–541. https://doi.org/10.1111/j.1468-2346.2010.00894.x.

ITU. (2009). Overview of Cybersecurity. Recommendation ITU-T X.1205. International Telecommunication Union. Retrieved from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDFE&type=items Accessed on April 22, 2024.

Klimburg, A. (2011). Mobilizing Cyber Power. *Survival*, 53(1), 41–60.

Kolet, K.S. (2001). Asymmetric Threats to the United States. *Comparative Strategy*, 20(3): 277–292.

Krekel, B.; Adams, P & Bakos, G. (2012). Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Report Prepared for the U.S.-China Economic and Security Review Commission. Northrop Grumman.

Lancelot, J.F. (2020). Cyber-Diplomacy: Cyberwarfare and the Rules of Engagement. *Journal of Cyber Security Technology,* DOI: 10.1080/23742917.2020.1798155.

Lango, H. (2016). Competing Academic Approaches to Cyber-Security, Conflict in Cyber Space: Theoretical, strategic and legal perspectives, edited by Karsten Friis and Jens Ringsmose, 7–26. London: Routledge.

Libicki, M. (1995). What is Information Warfare?, National Defense University. Retrieved from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662 Accessed on April 30, 2024.

Lieber, K. (2014). The Offense-Defense Balance and Cyber Warfare. Cyber Analogies, edited by Emily O. Goldman and John Arquilla. Monterey, California: Naval Postgraduate School.

Lindsay, J.R. (2013). “Stuxnet and the Limits of Cyber Warfare”. *Security Studies* 22(3): 365–404.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law and Policy*, Vol. 4(63), p. 63.

Mandiant. (2013). Exposing One of China’s Cyber Espionage Units. Retrieved from: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, Accessed on April 25, 2024.

Manson, G.P., III. (2011). Cyberwar: The United States and China Prepare for the Next Generation of Conflict. *Comparative Strategy* Vol.30(2),121–133. https://doi.org/10.1080/01495933.2011.561730.

Mearsheimer, J.J. (1990). Back to the Future: Instability in Europe After the Cold War. *International Security* Vol.15(1), 5–56.

Mearsheimer, J.J. (2001). *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.

Mearsheimer, J.J. (2006). "*Structural Realism". International Relations Theories: Discipline and Diversity*, edited by Tim Dunne, Milja Kurki, and Steve Smith, 71–88. Oxford: Oxford University Press.

Morgenthau, H.J. (1948). *Politics among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf.

Mulrine, A. (2016). How North Korea Built up a Cadre of Code Warriors Prepared for Cyberwar. Christian Science Monitor. Retrieved from: http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-acadre-of-code-warriors-prepared-for-cyberwar Accessed on April 20, 2024.

National Security Strategy. (2010 May). The White House. Seal of the President of the United States. Retrieved from:.

Ndzendze, B. & Marwala, T. (2023). *Artificial Intelligence and International Relations Theories.* Palgrave Macmillan.

Nye, J.S. (1990). "Soft Power". Foreign Policy 80: 153–171.

Nye, J. S. (2010). Cyber Power. Harvard Kennedy School, Belfer Center. Retrieved from: http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA522626. Accessed on April 30, 2024.

Nye, J.S. (2011). *The Future of Power*. New York: Public Affairs.

Reardon, R. & Choucri, N. (2012). The Role of Cyberspace in International Relations: A View of the Literature". Paper presented at the 2012 ISA Annual Convention, San Diego, CA. 1 April.

Reisinger, D. (2012). Obama Takes Cyber-warfare to New Level, Report Says. CNET News. Retrieved from http://news.cnet.com/8301-1009_3-57445275-83/obamatakes-cyberwarfare-to-new-level-report-says/ Accessed on April 28, 2024.

Rocha, M. (2019). The Cyber Issue and Realist Thinking. *Esc. Guerra Nav., Rio de Janeiro*, Vol.25 (2), 517-543.

Saad, S., Bazan, S., & Varin, C. (2011). Asymmetric cyber-warfare between Israel and Hezbollah: The web as a new strategic battlefield. Proceedings of the ACM WebSci'11, Germany. Retrieved from: http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf. Accessed on April 17, 2024.

Sanger, D. (2012). Obama Order Sped up Wave of Cyberattacks against Iran. The New York Times. Retrieved from: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all Accessed on April 26, 2024.

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: Public Affairs.

Spade, J. M. 2011. China's Cyber Power and America's National Security. The U.S. Army War College. Retrieved from: http://www.dtic.mil/dtic/tr/fulltext/u2/a552990.pdf. Accessed on April 30, 2024.

Snyder, G.H. (2002). Mearsheimer's World—Offensive Realism and the Struggle for Security: A Review Essay. *International Security*, Vol. 27 (1), 152.

Tabansky, L. (2011). Basic Concepts in Cyber Warfare. *Military and Strategic Affairs*, Vol. 3(1), 75-92.

The Comprehensive National Cyber Security Initiative. (2007). Executive Office of the President of the United States. Retrieved from: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf Accessed on April 22, 2024.

The National Strategy to Secure Cyberspace. (2003). The White House. Retrieved from: https://assets.documentcloud.org/documents/2700096/Document-16.pdf Accessed on April 20, 2024.

Thomas, T. L. (2009). Nation-State Cyber Strategies: Examples from China and Russia. In F. D. Kramer, S. H. Starr and L. K. Wentz, Cyberpower and National Security (pp. 477-486). Washington, D. C.: Center for Technology and National Security Policy, National Defense University Press, Potomac Books Inc. Retrieved from: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP Accessed on April 16, 2024.

Tofan, D. C., Andrei, M. L. & Dincă, M. L. (2012). Cyber Security Policy. A Methodology for Determining a National Cyber-Security Alert Level. *Informatica Economică,* Vol. 16(2), 103-115.

US Army Cyber Command. (2020). About Us. Retrieved from: https://www.arcyber.army.mil/Organization/About-Army-Cyber/ Accessed on April 23, 2024.

US Department of Defense. (2010). USCYBERCOM Fact Sheet. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf Accessed on April 12, 2024.

Valeriano, B. & Maness, R.C. (2016). Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes? Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives, edited by Jens Ringsmore and Karsten Friis, 45–64. London: Routledge.

Waltz, K.N. (1979). *Theory of International Politics.* London: Addison Wesley.

Waltz, K.N. (1990). “Nuclear Myths and Political Realities”. *American Political Science Review* Vol. 84(3), 731–745.

Copyrights