Article

China-US Cyber-attacks and International Security

Nnamdi Azikiwe Journal of Political Science (NAJOPS).
2023, Vol. 8(2)
ISSN: 2992-5924

ADENUGA, Asimiyu Olayinka
Department of Political Science,
Tai Solarin University,
Ijagun, Ijebu-Ode,
Ogun State, Nigeria.

ABIODUN, Temitope Emmanuel
Department of Political Science,
Tai Solarin University,
Ijagun, Ijebu-Ode,
Ogun State, Nigeria.

Abstract

Nations in the contemporary world are confronted with threats from multiple fronts. The threats are so enormous that it is virtually impossible to keep track of all of them. Cyber-attacks represent one of such threats in the international security domain. This paper examined mutual cyber-attacks between China and America - two competing major powers in the international system - whose actions and/or inactions in the cyberspace have grave implications on international security. Each has tried to present the other party as the culprit in cyber-attacks, while claiming innocence. This paper, using the historical method, interrogated such claims and examined the implications of the mutual attacks on international security. It found out that both countries are involved in mutual cyber-attacks and this portends grave danger to international security, particularly the fact that it can snowball into nuclear confrontation. The paper recommended that the two countries, rather than engage in mutual recriminations, should have frank discussion, including at the highest level, on how to deal with the issue. This will not only defuse tension but also build confidence between the two countries. As well, being leaders in cyberspace capabilities, they should spearhead a treaty that will ensure responsible use of the cyberspace, both between themselves, as well as in the international system. This will create a regime of ethical and legal use of the cyberspace.

Keywords

Cyber-attacks, Cyber infrastructure, Cyberspace, International security, Nuclear confrontation

Introduction

The contemporary international system is a highly networked world with linked computer systems undergirding services and infrastructures on a global scale. Individuals, groups, organisations and nations are connected via the internet. As at 2020, there were more than 50billion connected devices around the world (Perwej, Abbas, Dixit, Akhtar, Kumar, Jaiswal, 2021) and the increasing complexity of such cyber infrastructure has resulted into a number of devices being subjected to a lot of vulnerabilities (Phillip, Chen, and Zang, 2014). No doubt, digitised information systems have become a force for good, but they have also been used for malicious purposes. Nations in the contemporary world are confronted with threats from multiple fronts that it is virtually impossible to keep track of all of them. Cyber-attacks represent one of such threats within the international security domain. With this kind of threat, an individual in a remote part of the globe can inflict tremendous damage on the infrastructure or security

Corresponding Author:
Adenuga, Asimiyu Olayinka, Department of Political Science,Tai Solarin University, Ijagun, Ijebu-Ode.
Email: adenugaa@tasued.edu.ng

architecture of a country. Gone are the days when threats are limited to nations massing troops along borders in interstate threats and attacks (Tadjbakhsh & Chenoy, 2007). Security issues are no longer limited to state actors alone but also involve threats from different sources, both state and non-state actors. The threats also emanate from the cyberspace, the virtual arena in which information is stored, modified and exchanged through network systems and physical structures using electronic and electromagnetic spectrum (Goutam, 2015).

Owing to the importance of cyber security to a nation's security architecture, states have embarked on measures that will ensure that their security is not compromised. In this paper, the researchers focus attention on the issue of cyber-attacks as they relate to China and America, two competing nations that are major powers in the international system whose actions and/or inactions in the cyberspace have great implications on international security. As competitors, each has tried to present the other party as the culprit, while claiming to be the victim of attacks from the other party. The aim of this paper is to interrogate such claims and examine the implications of the mutual attacks on international security. Finally, the paper proffers suggestions on how the two nations, as major powers in the international system, can fashion out an order that will usher in a responsible regime of cyber security and ultimately international security. The paper is divided thus: introduction, conceptual clarification, theoretical framework, cyber-attacks between America and China, US-China cyber-attacks and international security, conclusion and recommendations.

Conceptual Clarification

There are two concepts that will be clarified here: international security and cyber-attacks.

International Security

Perhaps the best way to approach the issue of conceptualising international security is to understand "security" itself. The reason being that a thin line separates the two, and besides what may appear to be an internal security issue sometimes has international dimension. The term security is difficult to define that it could win universal acceptance owing to its multi-dimensional nature. The *Oxford Languages Dictionary* defines security as "the state of being free from danger or threat". While this captures an aspect of the concept, it is rather narrow considering its usage in the literature. To start with, security is multi-pronged in nature; it is not a unidirectional term as one would define an atom, energy or force in science. It is this multi-sided nature that rubs off on the "international" aspect of the concept. This understanding will be appreciated when one considers the various attempts by scholars to come to grips with the definition of the concept. Ulman (1983) defined security as decrease in vulnerability of a country. Even though the referent here is to a country, it is equally applicable to individuals, groups or the entire society. The essentialist conception of the term focuses attention on the core values to be protected. For example, Baldwin (1997) defined it as a situation in which there is low probability that acquired values will be damaged. Speaking in the same vein, Krause and Nye described it as "the absence of acute threats to the minimal acceptable levels of the basic values that a people consider essential to its survival" (1975, p. 330). National security definition by the Traditional school of thought conceives of it only in military terms and is generally associated with Cold War sentiments, what Buzan (1991, cited in Afolabi, 2015) typified as strategic reductionism and technical and mechanistic obsession with military balance and usage of cutting-edge technology. However, the inadequacy of this approach has been exposed owing to the fact that threat to national security can emanate from other sources such as hunger, unemployment,

poverty, etc. This made McNammara (1968) to assert that a country seeking national security without paying attention to critical issues of unemployment, poverty, hunger, as well as inadequate public utilities is living in a fool's paradise (Nwolise, cited in Afolabi, 2015). His view that security is inextricably linked with development and that development will remain a mirage without security is unimpeachable. To Buzan (1991, pp.432 - 433) security is "the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change, which they see as hostile." The essence of security is survival, including concerns about conditions of existence. While the definition is expansive on the idea of security, there is no objective unilineal way of identifying a "security" issue among the range of concerns about existential conditions.

The foregoing underscores the multiple lenticular perspectives of which the concept is viewed. Security here is viewed as the minimisation of threat to the well-being of an entity that is not a threat to other entities. The strength of this definition lies in the fact that it can apply to individuals, groups or nation(s), and what they regard as well-being, which is not a threat to the well-being of others. Taking a cue from the above discourse, international security is equally multi-dimensional. In the current globalised world, it can no longer be viewed according to the lens of the traditionalist as the military capability of a state to maintain its security. The reason for this is that threats to a state can come from multiple fronts to which bombs and guns are inappropriate to fight. For example, how does a nation deploy troops to counter threats emanating from the cyberspace? It is only countermeasures that are within the cyberspace that will be appropriate. It is the realisation of this that informs the conception of international security, not as a zero-sum game by states but as a multi-sum security principle involving five dimensions, viz: human, environmental, national, transnational, and transcultural security (Al-Rodhan, 2007). While human security focuses on the individual, the concerns in environmental security have to do with issues of climate change and access to resources. The third principle, national security, beams the searchlight on the ability of a state to exercise monopoly over the use of force as demonstrated in the country's policing and military capabilities. The fourth and fifth principles direct attention to transnational threats - such as terrorism- and impairment of transcultural security through real or potential threat to civilisational forms, respectively.

Perhaps, it is this Janus-faced and inscrutable nature of security that made Kolodziej (2005) to liken it to a Tower of Babel. International security actors can be individuals, groups, local governments, nations, non-governmental organisations, as well as the international system (Rothchild, 1995). Buzan (2007), also pointing to the broad canvas from which international security issues might emerge, stated that the issues do not just focus on threats to states but on the ones that can be tolerated and those that require immediate response or action. International security is seen as efforts and measures undertaken by bodies - nations, regional and international organisations - to ensure their survival and safety, whether through the use of diplomacy and/or military actions (Afolabi, 2015). In sum, international security can be defined as the sum of national and international organisation strivings to ensure the safety and well-being of the constituent units of the international system. This can only be assured when members of the international society reach a consensus on the rules of behaviour among its constituent entities and their practical implementation (Salmon, 1996).

The content of international security keeps changing as threats assume new dimensions. It is no longer focused on military concerns as it used to be under the narrow traditional state-centric approach. Today, it encapsulates all issues that border on the survival of states –economic, food, environmental, spread of

infectious diseases, religious, ethnic, ideological, energy, science and technology, human security, climate change, and activities of non-state actors, all of which are hardly stand-alone issues but cross-cutting and impinging on the security of the state (Buzan, et. al, 1998).

Cyber-attacks

What is a cyber-attack? It refers to "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself." (National Institute of Standards and Technology, n.d). It is also described as "any attempt to gain unauthorised access to a computer, computing system or computer network with the intent to cause damage" (Pratt, 2022, Cyber Attacks). The aim, according to Pratt, is to "disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems." From the above definitions, cyber-attacks can be summed up as criminal acts that occur within the cyberspace to harm, hobble, commit data heist or breach, and/or hack computer systems such that they are rendered inoperable temporarily or permanently. Cyber-attacks come in various shapes and forms (Gotham, 2015; Perwej, et al.; 2021; Prat, 2022) and they grow in sophistication with technological advancement. Perwej et al. detail many of these, but for reasons of scope and space, few of them are discussed here.

Cyber stalking occurs when individuals are harassed in the cyberspace by unknown persons. The attacker poses as one that is familiar to the victim, only for the purposes of harassing such individuals, leading to distress and fear on the part of the victim. In phishing particular targets are attacked in order to gain access to confidential information on such: passwords, account number, social security number, credit card number, etc. Variants of phishing include whale phishing and spear fishing. The former goes after the big fish in an organisation; for example, the Chief Executive Officer, or some key functionaries of the establishment, who invariably will be willing to pay ransomware because such would not want the organisation to be embarrassed by news that the body's cyber security has been compromised. In the latter, a specific target is deceived to get useful information for malicious purposes from the individual. This may lead to loss of hefty sums of money.

In identity theft, perpetrators steal the identities of their victims and commit crimes in their names. While posing as their quarries, they can buy goods online or commit other crimes. The Police will be after the innocent person without knowing that that it is a case of identity theft. Spoofing is an act of deception on the part of the attacker to make the target believe that the correspondence or messages are transmitted from a trusted source. Attackers tinkers with the IP address to make the message appear to come from a trusted website. There could also be infections with worms, Trojan horses, and viruses, which affect the computer system negatively. Worms require no supportive executable files before they can damage the computer. Viruses, on the other hand, require such, while Trojan horses are apparently useful software files but have backdoors through which malicious users can gain access to important information about individuals, groups or organisations.

As for Denial of Service attack, authorised users are denied the services of the server or network, hence delaying their activities. In case of Distributed Denial of Service, Denial of Service is simultaneously propagated by multiple systems, what is called botnets (Goulam, 2015). The purpose is to leave the victim exasperated and to make the repairs expensive. E-mail bombing floods the targets mail box with thousands and perhaps millions of e-mail messages such that the server becomes overwhelmed and crashes or the victim is unable to have access to important e-mails. Salami attacks occur when an

insignificant or imperceptible amount is stolen from the account of customers through a program written in the banking software that draws this amount from customers' accounts. Stealing such from thousands and perhaps millions of customers at the same time amounts to huge sums.

In Man-in-the-middle (MITM) attacks, the attacker eavesdrops on conversations or data sent between correspondents, networks or computers (Panda Security, 2023). The attacker stays in the middle to apprehend what goes on between the individuals or networks communicating with each other, actively spying on them and/or modifying the messages to suit some malicious purposes. Intellectual property theft is another form of attack. Intellectual property refers to innovations and new methods and models that have been patented. They are usually of high economic value. The internet, owing to its ability to mask users, is often used as a means of intellectual property theft. State-sponsored attacks represent another form of cyber-attacks. While there are lone wolf and group attacks, states themselves initiate attacks against one another for a variety of reasons: securing military, political, economic advantages; these attacks are usually sophisticated and difficult to detect. They sometimes involve exploiting the vulnerabilities of systems, software or programs before they are patched by the developers.

Other attacks are password attacks, including brute force attack, through which the hackers guess password of victims and Structured Query Language attacks, which replace a usual log-in or password to gain access to the system and compromise it. Some other ones are URL interpretation, through which hackers gain access to the site's back-end thereby getting information on users; DNS or Domain Name Spoofing in which hackers create a fake website and victims are made to send sensitive information to such, thereby making the malefactors to gain access to them. There are also insider attacks coming from those within the establishment who are familiar with the security architecture and who can make attempts to compromise same for selfish ends; drive-by attacks in which users are infected once they visit or "drive-by" the site. As for XSS or cross-site script attacks, the malevolent attacker designs malicious scripts using clickable content and transmits same to a browser. Clicking on the content will cause the script to be executed. Birthday attacks are based on the belief that in a room of 23 people, there is 50 percent chance that two birthdays will be similar, hence those who use birthday as their hash algorithm to check message authenticity may have their security compromised.

Methodology

The paper is essentially a qualitative work that adopts the historical methods. The paper made use of the historical method. In this regard, sources for the research were mainly secondary, including newsper reports, books, and the internet The historical method was considered suitable because it gathers evidence, examines whether there are loopholes in the evidence; in other words, it critiques it before telling the story (Mason, McKenney &Copeland, 1997). It is not just a chronological presentation of events, but one that is committed to systematic and objective presentation of facts. Given that this discourse involves parties that are engaged in mutual accusations and counteraccusations over time, then there is need for objective assessment of these claims with other sources, which represents a core aspect of the historical method.

Theoretical Framework

The theoretical framework that will be used to anchor this study is offensive neorealism as propounded by Mearsheimer (1994/95). Other scholars that hold neorealist views include Herz, Evera and Jervis. In order to bring to the fore the offensive realist theory, it will be necessary to provide a background of the

realist theory from which it springs and to which it is closely associated and compare it to defensive realists, thereby bringing to bold relief the essence of the theory. Neorealism takes its root from realism, which posits that the international system is anarchic in nature, hence in the absence of an overarching authority to control states' behaviour - as it happens within the domestic environment – they (states) resort to self-help to ensure their security. As states cannot assure their security by depending on benevolent actors within the system, it behooves them to aggrandise their power so as to checkmate aggressors. This conception of the international system provides the basic stuff for neorealism, an offshoot of classical realism. However, its point of departure from classical realism is that it does not subscribe to the selfish or evil nature of man as the driving force of inter-state relations within the international system, rather it is the anarchical nature of the system itself that drives states' behaviour. In essence, the neorealist theory, according to Mearsheimer, 1994/95) is based on the following assumptions: the international system, with great powers as the major actors, is anarchical in structure; that is, no overarching power to mediate conflicts and punish offenders; offensive military capability which all states have can dispose them to harm others; states cannot gauge intention of other constituent units; survival as a motive force drives actions of member states in the system, which in turn determines the strategies employed by these states as rational actors in the system (Steinssson, 2014).

While all neo-realists share the above assumptions, there are disagreements between the offensive neo-realists, as represented by Mearsheimer (1994/95), and defensive neo-realists, as exemplified by Kenneth Waltz (1979). Whereas the assumptions above are seen as given, the neo-realists argue that the anarchical nature of the system makes states, in particular the major powers, to act as power maximisers, hence the "the world is condemned to perpetual great power competition" (Valeriano, 2009) suffused with hegemonic intentions by the states.

Certain criticisms have been levelled against the neo-realists. In contradistinction and as a criticism of the neorealist position, defensive neorealists argue that hegemony would only lead to other states taking counterbalancing measures in order to ensure that the status quo is maintained. Besides, offensive realism is an expensive measure not only in term of cost, but in terms of pacifying the conquered. Maintaining existing infrastructure and rebuilding those destroyed can tax the resources of the hegemonic power beyond measure. Nationalism among the conquered is equally a sentiment that can hardly be conquered by bayonets and bullets or rockets and missiles. Given this scenario, therefore, hegemony as posited by the offensive realist is hardly justified by the costs it incurs for the hegemon. In place of offensive realism, defensive realists posit that states seek security by ensuring a maintenance of the status quo via balancing, which is more common than bandwagoning (Waltz, 1979).

On the question of application, neorealism applies here because the two powers are seeking to gain advantage over each other. While the United States enjoys dominance currently in the cyberspace, China seeks to catch up and eventually overturn America's supremacy in the domain, hence the resort to cyber-attacks, among other measures. It is this rivalry that colours their relationship in the cyberspace which, given their leading positions in the cyber realm, poses a lot of danger not only to their economies but to international security as we shall soon see in subsequent sections.

Cyber Attacks between America and China

Both China and the United States of America have accused each other of being behind the attacks on their countries. In the SHADY RAT incident in 2011, a large number of corporations, international

institutions and governments in America, 72 in number, were targeted in order to extract state secrets, weapons' technology, businesses intellectual property and others of strategic importance, what some have dubbed the largest theft in history (Sanger and Markoff, 2011). In 2021, Microsoft, a giant American corporation was attacked. Hackers were able to access thousands of American corporations, stealing passwords in these organisations through the backdoor (Brodkin, 2021). Not only that but also the National Aeronautics Space Administration website and that of Google have been attacked in similar manner. In all these, America has continued to point accusing fingers at China. An exasperated Wray, the US Federal Bureau of Investigation Director, lamented that Chinese government had stolen staggering volumes of information causing job-destroying damage across a lot of industries in the country (Jaupi, 2021, February 3). He stated further that China had carried out cyber-attacks against America more than any other country with over 2,000 such attacks under investigation.

In their ounteraccusation, Chinese officials claim that it is their security space that has suffered relentless onslaught from attackers, with the United States being the greatest culprit, and that China has been the target of some 34,000 cyber-attacks from the US (Xinhua News, 2009). Recently, too, China's National Computer Virus Emergency Response Center (CVERC) accused the US NSA-affiliated Tailored Access Operations (TAO) Office of using 41 types of cyber weapons in one of the cyber-attacks against China's Northwestern Polytechnical University with more than 140 gigabytes of data stolen in more than 10,000 cyber-attacks (China.org.cn, 2022, September 12),

Where does the truth lie between the two recriminating nations? The fact is that both countries are guilty of carrying out cyber-attacks on each other, hence the kettle should not call the pot black. Chinese citizens have been found guilty by US courts on cyber espionage (Jaupi, 2022) and China has been accused of copying a lot of technology of the West, particularly America, illegally (Clayton, 2014). Some Chinese intellectuals have been caught doing so. It is also a fact that 40% of the 50 internet-spewing service providers are found on the soil of the United States. State agencies like the NSA engage in cyber operations, while the US or its allies control all the 13 of the root servers that make smooth operation of the internet possible (o'Flaherty, 2019). Apart from individuals and groups that carry out lone attacks, both countries seek to compromise the security of each other in the cyberspace. The reason for this is that both of them are rivals in the international system and, in a neo-realism fashion, seek to undo or outdo the other for the purpose of securing advantages that will enhance their power in relation to the other party. Politically, the United States of America seeks to trump the communist ideology and spread democracy everywhere, one value they believe should have universal application. Therefore, seeking to undermine the communist ideology and replace it with democracy sits well with the country. So, ideological supremacy is one motivating factor on the part of the United States of America. The Americans have reasons to hope for an eventual overthrow of communism in China. One, they succeeded in dismantling the Communist regime in the former Soviet Socialist Republics. Two China has embraced a measure of capitalism, the twin ideology that United States democratisation process seeks to promote. Three, America works assiduously to remain the lone super power of the world having succeeded in attaining this status following the dismantling of the Soviet Union from 1991 onwards. Its officials pride themselves as the greatest military power in the international system.

China, on the other hand, appears to be playing the catch-up economically, militarily, in science and technology, etc. It has set the goal of 2050 as the time it would have attained the power of the greatest nation on earth (Shi, 2017, October, 17). To do this, the Chinese have made it a state policy to bridge that

gap and surpass America economically, militarily and in science and technology. China and the United States of America are not only political rivals, they are equally military competitors. America has its tentacles around the world in terms of setting up military bases. That is to give teeth to its policy as the policeman of the world. Its tentacles spread across the Western Hemisphere, Asia, Africa, Middle East, etc. China, particularly since the emergence of Xi Jinpin seeks to challenge that dominance and have its influence spread around the globe. It seeks to be the sole arbiter of what goes on in the Southeast Asian corridor. For this reason, it has taken pre-emptive steps of developing an artificial island, re-jigged its navy to thwart challenges and its competitor's moves in the area. All these directly challenge the influence of the US and its allies such as Japan and Philippines. Besides, as a new entrant to global superpower competition and to secure itself militarily, China has developed intercontinental missile capability and delivery systems. It has even gone to surpass the United States in developing some of these weapons systems. A notable example is the hypersonic systems, which it developed earlier than the United States. The blueprint of some of these systems were made by the US but not developed and are stolen by the Chinese, of course through instigating a breach of the cyberspace of the former.

US-China Mutual Attacks and International Security

What danger do the mutual attacks portend for international security? The international system is such that an incident in one country or a group of countries has reverberating effects on the entire system. Witness the collapse of the financial system in the US in 2008 that affected the entire globe. In like manner, US-China cyber-attacks portend a lot of dangers to international peace and security in the following ways. As reported by Richie (2023, May 25), a British Broadcasting Corporation (BBC) journalist, Chinese hackers used stealthy malware to attack US bases in Guam. The bases serve strategic purposes, particularly in responding to conflicts in Asia for America and its allies. A crippling of the infrastructure represents not only a threat to America but its allies, hence the international dimension of the security threat. Cyber-attacks on critical infrastructure can snowball into mutual attacks on weapon systems. As observed by Fox (2022), in this digital age, cyber-attacks can shut down nuclear power plants. Knowing fully that the two countries are nuclear superpowers, confrontation by the two countries could escalate to nuclear attacks, which might effectively mean the end of civilisation. A nuclear confrontation has the potential of spillover effects on other countries apart from the belligerent states. The fallout of nuclear bombs will be carried by winds and rivers or seas making such a threat to other countries. Therefore, nuclear attacks cannot be localised in their effects even if there is no immediate threat of nuclear Armageddon because both parties observe restraints not to embark on an all-out nuclear attack.

In the area of trade, since nations are interdependent, mutual antagonistic cyber-attacks will have negative implications on smooth running of trade operations. Where critical goods supply is targeted, for instance, that means that such will not be available to other nations. Take for example, wheat supply. Where this is disrupted, food security is compromised for other nations apart from the antagonistic nations. That happened, for example, in the recent Russia-Ukraine war. Inflation could result leading to food riots and other forms of instability in those nations affected by disruption in food supply. An interruption of gas supply due to cyber-attacks on flow stations, say in winter, will cripple critical supply that may lead to thousands of deaths. Other critical infrastructures may be crippled, too. Cyber espionage, particularly in the area of intellectual property will cause either party to experience great loss amounting to billions if not trillions of dollars. The estimated cost of cyber-attacks for the global economy in 2021 has been

put at $6trillion dollars (Perwej et al., 2021). A tit-for-tat approach by the two countries will no doubt harm their economies in no small measure, which will have devastating effects on the economy of other countries owing to the interdependence of nations. China is regarded as the "world's factory" and global supply of goods could be affected if the two countries seek to attack each other's infrastructure.

Conclusion

The paper has examined the concepts of cyber-attacks, as well as the mutual effects of these on the two leading but antagonistic superpowers in the cyberspace, on the one hand, and the potential impact that the attacks portend for international security, on the other. It was established that attacks by one of these nations may provoke attacks on other sectors, leading to a hybrid warfare, which consequences might be difficult to predict. International security could be seriously harmed by tit-for-tat attacks by the two leading cyber superpowers.

Recommendations

Given the above scenario, the following recommendations are proffered. The two countries should spearhead a treaty on the responsible use of the cyberspace through which issues of cyber security can be ironed out. Treaties have helped to ensure relative stability in certain aspects of international relationships, for instance in strategic arms limitation (SALT I and SALT II), between US and Russia. It will not be out of place if an international treaty can be fashioned out to which countries can key into. It is not likely that this will be a hard sell as all countries are exposed, both potentially and/or actually, to cyber threats that could harm their critical infrastructure and, by extension their security. In a Reuters report (Satter, Siddiqui & Pearson, 2023, May 26), America issued an advisory to its allies – Britain, Canada, Australia and New Zealand - that their critical infrastructures, including oil and gas and rail systems, could be attacked because China possesses the capability to do so, and that it has been spying on the infrastructure lately using Volt Typhoon to break into their networks. Such a report underscores the need for countries to join hands in dealing with the menace of cyber-attacks on a global scale.

Presently, there is trust deficit between China and America, owing to mutual recriminations on cyber-attacks by state-sponsored operatives in both countries. There is the need to take up this issue at the highest level, say during state visits. Frank discussion as to how to deal with the issue will serve not only to defuse tension but also to build confidence and make a way for discussion about creating norms for responsible use of the cyberspace. The two countries, being leaders in cyberspace capabilities, should also be in the van of making rules at the United Nations that will usher in a regime of ethical and legal use of the cyberspace. Countries breaching these rules should not just be excoriated but sanctioned by the targeted states, and if incapable to do so owing to relative weakness, by the UN, once a treaty to that effect has been put in place. Under the Obama administration, when Xi Jinpin was on his first visit to America, researchers and intelligence officials noted that the threat of sanctions on China for cyber-attacks led to a significant drop in hacking activities traced to the country (Perlroth, 2021, July 19). There is also need for further technological development, particularly in quantum computing, which will make cyber breaches harder to carry out.

References

Afolabi, M.B. (2015). Concept of security. In K. Ajayi (Ed). *Readings in Intelligence and Security Studies* (pp.1-11).Ado-Ekiti: Department of Political Science and International Studies, Afe Babalola University. Retrieved from https.//www.reseachgate.net

Al-Rodhan, Nayef, R.F. (2007). *The five dimensions of global security: Proposal for a multi-sum security principle.* Berlin: LIT Verlag.

Brodkin, J. (2021). US warns China over state-sponsored hacking, citing mass attacks on Exchange. Retrieved from US warns China over state-sponsored hacking, citing mass attacks on Exchange | Ars Technica).

Buzan, B. (1991). New patterns of global security in the twenty-first century. *International Affairs*, *67*(3),431.

Buzan, B. (2007). *People, states and fear*. Colchester: ECPR.

Buzan, B., O. Wæver, O., Wilde, J. (1998). *Security: A new frame work for analysis*. Boulder, Colorado: Lynne Rienner Publishers

China.org.cn, (2022, September 12). Chinese reports uncover details of cyber-attacks by US security agency. Retrieved from Chinese reports uncover details of cyber attacks by US security agency - China.org.cn

Clayton, M. (2014, May 19). US indicts five in China's secret 'Unit 61398' for cyber-spying. *Christian Science Monitor*.

Goutam, R.K. (2015). Importance of cyber security. *International Journal of Computer Applications (0975 – 8887) 111* (7), 1-4.

Fox, J. (2022, October 7). 8 biggest cybersecurity attacks in history. Retrieved from https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history

Guterres, A. (2022). Threat to global security more complex, probably higher than during Cold War, Secretary-General warns Munich Security Conference. Retrieved from https://www.un.org/press/en/2022/sgsm21146.doc.htm

Jaupi, J. (2021, February 3). FBI – China cyber-attacks on USA. Retrieved from https://www.the-sun.com/tech/4604553/fbi-china-cyber-attack-united-states/

Kolodziej, E. (2005). *Security and international relations*. Cambridge, Cambridge UP

Mason, R.O., McKenney, J.L., &Copeland, D.G. (1997). An historical research for MIS research: Steps and assumptions. Retrieved from https://www.jstor.org/stable/249499

McNamara, R, (1968). *The essence of security.* London: Hodder and Stoughton

Mearsheimer, J. J. (1994/1995). The false promise of international institutions. *International Security* 19(3), 5-49.

National Institute of Standards and Technology (n.d). Cyber-attack. Retrieved from https://csrc.nist.gov/glossary/term/Cyber_Attack

O'Flaherty. (2019). NSA launches cybersecurity arm to defend the US from foreign adversaries. Retrieved from NSA Launches Cybersecurity Arm To Defend The U.S. From Foreign Adversaries (forbes.com)

Panda Security. (2023). What is a Man-in-the-Middle (MITM) attack? Definition and prevention. Retrieved from https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/

Peltroth, N. (2021, July 19). How China transformed into a prime cyber threat to the U.S. Retrieved from. Retrieved from https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

Perwej, Y, Abbas, S.Q., Dixit, J.P., Akhtar, N., Anurag Kumar Jaiswal, A.K., (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management (IJSRM) 9* (12), 669-710.

Philip, C. L., Chen, O., & Zhang, C. Y. (2014). Data-intensive applications challenges techniques and technologies: A survey on big data. *Information Sciences, 275*, 314-347

Prat, M.K. (2022). Cyber-attacks. Retrieved from What is a cyber-attack? Definition, examples and prevention. TechTarget

Ritchie, H. (2023). Microsoft: Chinese hackers hit key US bases on Guam; Retrieved from https://www.bbc.com/news/world-asia-65705198

Sanger, D.E., & Markoff, J. (2011, June 11). I.M.F. reports cyberattack led to 'very major Breach.' *New York Times*. Retrieved from http://www.nytimes.com/2011/06/12/ world/12imf.html

Salmon, T.C. (1996). The nature of international security. In R. Carey, T.C. Salmon. (Eds) *International security in the modern world*. London: Palgrave Macmillan,

Satter, R., Siddiqui, Z., & Pearson, J. (2023, May 26). U.S. warns China could hack infrastructure, including pipelines, rail systems. Retrieved from https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/

Shi, T. (2017, October 17). Xi plans to turn China into a leading global power by 2050.Retrieved from https://www.bloomberg.com/news/articles/2017-10-17/xi-to-put-his-stamp-on-chinese-history-at-congress-party-opening#xj4y7vzkg

Steinssson, S. (2014). John Mearsheimer's theory of offensive realism and the rise of China. Retrieved from https://www.e-ir.info/2014/03/06/john-mearsheimers-theory-of-offensive-realism-and-the-rise-of-china/

Tadjbakhsh, S., & Chenoy, A. (2007). *Human security: Concepts and implications*. NY: Routledge.

Ullman, R. (1983). Redefining security. *International Security 8*(1), 129–153

Valeriano, B. (2009). The tragedy of offensive realism: Testing aggressive power politics models. *International Interactions, 5*(2), 179 -20

Waltz, K. (1979). *Theory of international politics.* Reading, MA: Addison-Wesley

Xinhua News. (2009, April 10). China is the biggest victim of spyware, most attacks origins from US. Xinhua News