IMPORTANCE OF CYBER EDUCATION IN THE ERA OF CYBER WAR

Syed Shahab Uddin
Assistant Professor,
Department of International Relations, FUUAST,
Sindh, Pakistan
Email: shahabhashmi2012@gmail.com

ABSTRACT
Cyber education is now a very important topic of concern in the world. It is also very important to keep our students up to date with the latest technology and the current happenings around us. Our kids nowadays are born in the digital age where we can use computers and the internet for our daily purposes and we are 24/7 engaged in different types of technologies. We can see that there are several things in which we are using this digital technology, so to comprehend all the new things we need to include these technological innovations and advancements in our education level from school to college to higher education. The research is a qualitative analysis of the significance of cyber education in today's cyberwar era. Multiple published types of research are examined in fulfilling the desired research objectives.

KEYWORDS
Cyber education, cyberwar, digital weapons, cyber security

INTRODUCTION

The term "cyber" refers to activities using computers and the electromagnetic continuum, Intranets, smartphone technologies, fiber optic wires, and outer world space communications are all part of the cyber domain, which means that cyber terms do not just consist of the internet source. In this cyber era, the information is very unsafe people with expertise in it will extract information about anything so quick and easily. (Nye, 2013) Cyber domain is a man-made complex atmosphere, because of the low entry barriers of the cyber world small nations and non-state actors can perform large action in it. May Great governments have more resources in cyber than non-state players, but it also costs more liabilities, and at this point in the technology's evolution, the attack is more important than defense in cyberspace.

If we talk about cyber education, we can see that cyber education initiatives, training, and programs are growing at an exponential rate. To boost the cyber education a program is launched known as CEP (cyber education project), CEP is sustained by a

group of diverse computing professionals of academic organizations and professional communities to give accreditation and form undergraduate programs in the discipline of cyber sciences. The field "Cyber Sciences" stands for the mixture of different computing-based fields such as technology, communication systems, network operations, risk, and management. Law, policy-making, and human resource also comes under the term of cyber sciences. One of the most important aspects is different strong nations adapt and include cyber education in their military academies. In 2012, America established MACEWG (Military academic cyber education working group) to develop undergraduates programs about cyber education for academics of the country's military (Sobiesk et al., 2015).

Digital crime and cyber terrorism are on the rise all around the world. The Internet has evolved into a new battleground, yet it appears that a large percentage of people are defending rather than aggressive (Dawson & Omar, 2015). The emphasis of the course is on safeguarding cyberspace rather than causing harm. Because colleges are where technologists get their start, they need to offer more provocative material. The worry of creating a malicious hacker must be replaced with a cyber-professional who is well-versed in all aspects of cyber warfare. If the United States intends to continue major participant in cyberspace, professional exercise must fundamentally shift and become a new norm. Because there aren't enough citizens, a fast track program might be implemented, precisely what individuals that participated in American president Bush's Iraq Invasion in 2005, experienced. (Wong, 2005). To develop offensive security education, after the (NICE) Cyber-security Professional Guidelines, another system must be proven. (Dawson, M. 2020)

RESEARCH OBJECTIVE

1. To recognize the importance of cyber education in the contemporary era
2. To identify the different dynamics of cyber war in present times
3. To uncover different techniques used in the cyber warfare

RESEARCH METHODOLOGY

The study is a document analysis of previously published articles on the related theme. It is based on secondary sources of research and qualitative methods are also utilized in this study. It is basically focused on the diverse domain of cyber world and it's related technologies.

LITERATURE REVIEW

Cyber Era: Shifting of World towards Cyber Technology

Nye (2011) in his book "The Future of Power" stated that one of the biggest shifts of this era, is the spread of power away from governments, and cyberspace is a wonderful example of this threat. The dominating and powerful nations of the world are unable

to control or gain the authority of the cyber world in the same way that they have dominated other world powers such as air, sea, and space. Libicki (2011), said that cyber domain researchers are still not sure what offensive, defensive, deterrence, and ammunitions control means in the cyber world, whereas Rid mentioned the threat of exaggeration of cyber-attack and suggested not to create hype about the cyber risk. The time is far away when big nations of the world agree to tackle matters of cyber security together and prepare for cyber combat. For example, to minimize the cyber risk, Russia and America mutually agreed to form numerous cyber security links.

Syed and Khaver (2019) state that like the rest of the world Pakistan also has to counter the threats from the cyber world. In Pakistan's case, cyberspace becomes an important part of banking institutions, academics, government, and armed forces department, and the telecommunication sector also.

According to Rasool (2015), Pakistan is slightly unable to safeguard its technical parameters. Pakistan is still unable to create a proper system to guarantee its safety from threats of the cyber domain. It turns out to be Pakistan's national security threat as the confidential information of government and individuals is at risk. Hacktivism becomes a major problem for Pakistan. Hackers are damaging, thieving, and exploiting the personal information of Pakistan's government. In Pakistan political extremism and terrorism is the major reason for increasing hacktivism. Because of the lag in cyber technology Pakistan is an easy target for cyber terrorism. Pakistan has to pay proper attention to cyber technology and work efficiently to make a strong position in the cyber world.

Many talented people are involved in unethical hacking activities, the government should utilize the skills of such people in a positive way to safeguard the cyber position of Pakistan. Computer education must become a mandatory course in schools and universities, so the coming generation is aware of cyber technology and tackles cyber threats. Pakistan should establish proper governing bodies that implement cyber laws and punish strictly those who breach the laws. Pakistan should sign treaties with powerful nations for cyber security, they can aid Pakistan to protect its digital system and Pakistan can also take advantage of the modern technology of developed nations to secure from cyber-attack and make progress in cyber technology.

Importance of Cyber education

According to Jaitner and McDermott (2015), everyday nations are accepting the fact that academics plays a vital role in the prosperity of a country's cyber department. Countries have started investing hugely in the programs related to the cyber domain, endorsing education exchange programs with countries, and also trying to improve and grow the cyber department in industries. Human-made cyberspace hugely depends on

different engineering disciplines such as engineering electric, engineering of computer and energy technology, Nanotechnology, telematics, and biotech. Cyber education mostly focuses on computer education. We can see many universities and colleges offering degrees and courses in the discipline of cyber security. Technology is the main element of cyber security, nations with a great hold on technology prove as great in the field of the cyber domain. West is way ahead in cyber education, Europe put even law and management in the cyber world such as ethical hacking. Power (2007), states that the west also includes managerial courses in cyber education such as project management and cost-benefit analysis. England also an emphasis on cyber strategy, United Kingdom believes that cyber security can be improvised by providing improvised knowledge of cyber education to both the civilian and the military. Cyber defense and cyberspace operations are the two major programs offered by Cranfield University. According to Saydjari (2004), an organically major part of cyber education consists of computer sciences and engineering.

Moon et al., (2008) stated that the cyber environment is coming as a new era of cyberinfrastructure to back the scientific research and education of the 21st century. The cyber environment is to visualize and analyze the stimulating occurrences by a combination of hardware, services, and tools. The cyber environment serves as an area for hardware resources and can also work as portals. A project e-AIRS is launched in the cyber environment. E-AIRS is a portal system based on cyberinfrastructure to deal with the process of aerodynamics engineering, this is an initial step of forming a cyber environment. This system helps the students to learn about the process of aerodynamics in a whole different way and similarly can be utilized in different fields of engineering such as civil engineering.

Contemporary concepts of the Cyber world

According to Akimova et al., (2019), the chapter defines the idea of a ‘Cyber Economy’ as an innovative economic system. The goal of this is to properly assess the early outcomes of the digital revolution in the contemporary economy, as well as the development of the concept of the cyber economy as a new type of economic system that will emerge as a result of digital transformation. They also describe the term "cyber economy" and scientifically define the reason and order for moving to the new digital model. Systems in which machines communicate with each other and with individuals are known as cyber-physical systems—will be the goals of administration in the cyber economy. The majority of respondents believe AI is a very harmful component of the cyber economy. The following are the key reasons under which the digital and cyber economy improve the standard of life and living principles: entrepreneurship; general policies to recompense the staff as robots replace human labor; a shift in the educational model to concentrate on the expansion of intellectual skills, beginning with before school learning; free charge creation for technologies that

adds to stop improve human resource, this will throttle innovation and drive up costs. The cyber economy will emerge because of the digital transformation of the existing economy, which will be built on Industry 4.0 breakthrough technologies. Within cyber-physical systems, it will show intimate connections and relations among people and intelligent machines, with maximized clearness, certainty, and controllability (Kovazhenkov et al., 2019).

The world is changing, and every change comes with advantages and disadvantages. In the cyber era, numerous factors are working for this shift, where communication and global networking are the main working factors. Information technology is the reason for speeded communication and global networking. Democracy can be defined as the government of people for the betterment of people. Cyber democracy comes into existence because of the birth of cyberspace. Cyber democracy is a term that can be used to define the relationship between information technology and the operations of democracy. Cyber democracy is also termed E-Democracy which is a lot related to technology revolutions, it is the future of democracy. Many authors labeled cyber democracy as direct democracy as the participation of citizens is of a very high level in it. Cyber democracy strengthens the position of citizens and increases their participation in democratic processes. (Barth, 2014) The danger of cybercrime is also very high in cyber democracy, as the information can be easily stolen and misused. As cyber democracy came into existence, future wars will be happening by digital attacks on a nation's democracy. Cyber democracy also compromises the freedom and privacy of governments and individuals, as it is almost impossible to erase data from the internet. In cyber democracy, the transfer of information becomes cost-efficient, because of the new media the information travels among the people faster with better quality.

Hua and Bapna (2013), have characterized cyber terrorism as a different method used by extremists to target cyberspace that is an addition to common terrorism. Computer fanatics will teach their people or hire from outside, according to FBI Director Robert S. Mueller, to mix physical and cyber operations. Mueller also stated that the government cannot fight the cyber threat alone. Cyber terrorists acquire not only terrorist tendencies but also hacker ones. Only by determining the purpose or aim of the individual or group conducting the assault can cyber terrorism be distinguished from ordinary hacking and other cybercrime (Tehrani, 2013). Cyber terrorism is defined as assaults carried out by cyber extremists by utilizing information systems to severely disrupt the governmental, societal, or financial operation of a vital group or institute inside a nation, or incite physical aggressiveness to hurt and cause casualties. Even though the phrase "cyber terrorism" is being used more frequently these days, there has yet to be an agreed-upon definition. In truth, amid the various definitions for cyber terrorism, some consistency might help us better comprehend the difficulties

surrounding cyber terrorism.

There have been serious offensive strikes against US infrastructure and corporations. Every week, a large information data break occurs, whereas reports substantial shortage of cyber security personnel continues to rise. Universities in the United States are hurrying to employ academics and create new labs to attract and keep students paying attention to pursuing a career in this field of cyber-security. According to (FISMA) study, the number of assaults is increasing while many agencies lag in implementing effective security. (Gikas et, 2010).

Humanity has conducted war throughout history to advance national objectives in an ever-changing international power struggle. Technology is continuously driving this game of power to move and adapt, from previous sword clashes to today's unmanned drone strikes. Armored vehicles, planes, and ships, as well as the usage of microchip technology & Telecommunications completely increased in the fighting zone & brought new & imaginative techniques toward improving edge over adversaries. The creation of cyber-space has fresh strategic opportunities & challenges triggering a rush to achieve a dominating situation intimate it, similarly to how flight's technical advancement sparked a competition to conquer the airspace (Mali, 2018).

Industrialization, mass manufacturing, and the advancement of science all contributed to the transformation of warfare. They might consider the Internet to be the most recent advancement in army technology. The development of order and control, just as the decline of uncertainty that causes the Clausewitz Ian "fog of war"- the uncertainty and disarray that hampered commandants during fights changed how fights are led. We know for a fact that an arranged power is more compelling than a comparative estimated non-organized power. Networked air defense is far more effective than air defense which is made up of a separate unit. States using data-connected (armored automobiles) (air jets) and (crafts) will battle efficiently with those who depend exclusively on power. Military networks have become legitimate and desirable targets as a result of their increased efficacy. The employment of network technology and cyberspace exploitation for intelligence and assault has become routine in military operations (Clausewitz, 2008).

Cyberspace

There are four components of cyberspace that include, and cyber-space is more than simply pc data info and knowledge. (Libicki, 2009)

A functional space: Individuals and cooperation use the internet to perform and create results, regardless of whether in the internet domains.
A natural domain: Cyber-space is a naturalistic sphere completely of electromagnetic

phenomena that can only be accessed through the use of computer technologies. *Cyberspace is founded on info:* people use it to generate, store, edit, trade, & exploit data.
Interconnected networks: The presence of links that allow electromagnetic activities that transport data.

A worldwide space inside the data surroundings that particular & irreplaceable atmosphere is outlined throughout the utilization of hardware & electro-magnetic range that make (store), (transform) (trade) & take advantage of data through related and interconnected organizations utilizing data correspondence advancements (Kuehl, 2009) .

Cyber war

Every individual, whether a fighter, a relative of an opponent, a member of the public, a commercial organization, or else a state, is affected by conflict and war in some way. As a result, cyber warfare research is both important and necessary to address the expanding number of difficulties generated by this new realm of conflict. (Robinson, 2015). Government authorities in the United Kingdom also worried about a deficiency of cyber warfare preparation and proposed additional investments to strengthen the defense, including the Public Cyber Security Program UK 'taskforce' over military digital attack risk, mps caution 2013. NATO has additionally been helping mindfulness, delivering the Tallinn Manual on International Law Applicable to Cyber Warfare (Schmitt, 2013) trying to help nations on the proper behavior legitimately in this new field of fighting. With this information in hand, it is evident that cyber warfare is a worldwide problem.

"Through the use of information technology to interrupt the activity of a government or organization, particularly the purposeful attack of communication networks by another state or organization," according to the definition given for cyberwar (Oxford English Dictionary, 2013). This definition, like the others under consideration, might be considered to be problematic. To begin with, it is unknown why electronic communications are being prioritized. Numerous frameworks can be in danger from digital fighting, including basic public foundation, for example, it influences lattice & conveyance of organizations (Nicholson et al., 2013). Furthermore, an attestation that digital conflict & digital fighting remains equivalent can be tested, the word reference himself gives goes against proof. Rather than characterizing the surely known and set up term of fighting as one more phase is used for war it characterizes the "Commitment in or the exercises engaged with war or struggle" (Oxford, 2013).

Cyber weapons

Cyber weapons pose several issues, including defining what a cyber-weapon is, how

it differs from traditional weapons, and whether or not it is feasible to govern their development and usage. A traditional weapon, according to Arimatsu (2012), is "a device meant to kill, harm, or cripple people, or to damage or destroy property. She guarantees that this depiction doesn't matter to digital weapons because the objective of a digital weapon is now and again to create an aberrant active effect that could conceivably bring about death, injury, or harm. To put it another way, cyber weapons like malware may be designed to just enable data collecting or establish a backdoor for future strikes. The concept that a cyber-weapon may describe as spiteful software with invasive capabilities, is not detailed enough to allow legal control. Arimatsu concludes that both capability and purpose must be considered when defining cyber weapons. Accordingly, a piece of malware or an instrument turns into a digital weapon just when it can incur hurt and the individual who utilizes it expects to do as such.

Cyberweapons have the potential to do more than just disrupt networks; they may also cause physical harm. A remotely communicated instruction, for example, led an electrical generator at the Idaho National Labs to self-destruct during the Aurora experiments. Digital assault should be visible as a second long attack weapon—quicker as rockets as well as aircraft, not so devastating, although less costly & perhaps undetectable. Depending on its goal, digital assaults might have significant or significant implications, including differing geopolitical ramifications, acceleration, and worldwide assessment. Therefore, all significant militaries have it however from the capacity to train unmistakable frameworks to breakdown. As of now, the chance of destruction, demise, and total damage digital attack is little. The attack that forces an originator to self-destruction could produce actual harm & maybe fatalities, although this could be minimal. (J. Meserve, 2007)

DISCUSSION

With time and the advent of new technologies people nowadays are exposed to higher threats from hackers. The nature of these threats is also very different from the past in which we cannot see or even know the person who is harming us. This is all done through the use of digital technology in crime that's why today's Era is considered the era of Cyber War.

In the education sector, this cyber technology is also very important and the knowledge about cyber education is also very significant because this cybercrime also threatens the educational sector of the country we also know that these cybercrimes are gaining ground in the education sector because these schools colleges and Universities are also vulnerable places in terms of the cyber-attacks.

Cyber education is also very important to safeguard the data from the criminals who are using these cybercrime techniques. For this, cyber security techniques are also very

vital to keep our important data safe from dangerous hands. Because, if we do not secure your data, it will be theft and the losses will be irreparable. According to some research reports, one in every fourth student in the US is experiencing theft or fraud before they reach the age of 18. So, in the world today cyber education is very important to save our children from being trapped in unsafe hands.

RECOMMENDATIONS

1. Since the world is more technologically advanced so cyber education should be given its due importance in the field of research and academia.
2. The government should make effective policies related to Cyber education.
3. Nowadays the nature of crime and criminal has been modified, so the cyber warfare techniques should be understood clearly and the general public should be aware of these techniques.
4. The overall population should be conscious of the mechanized techniques of the Cyber War by keeping oneself alert to its hazardous impacts of cybercrime and criminals.
5. Cyber education should be chosen as a career opportunity. In the future, the world is changed and the inclusion of the Cyber Technology Revolution revolutionizes the existing system.
6. The government should be aware general people from cyber thefts, damages, and other types of cybercrimes through public service campaigns.
7. In this cyber age, hackers and cyber terrorists have endless opportunities to exploit the citizens, so knowledge related to cyber education is a key in the coming future. Policymakers should also think about this issue.
8. Cyber security should be established as a separate field of study in higher educational institutes.

REFERENCES

Akimova, O. E., Vitalyeva, E. M., Ketko, N. V., Rogachev, A. F., & Skiter, N. N. (2019). The methodology of decision support for the entrepreneurial sector in the information asymmetry of the cyber economy. *In The Cyber Economy* (pp. 233-251). Springer, Cham.

Arimatsu, L. (2012, June). A treaty for governing cyber-weapons: Potential benefits and practical limitations. In *2012 4th international conference on cyber conflict (CYCON 2012)* (pp. 1-19). IEEE.

Barth, T. D., & Schlegelmilch, W. (2014). Cyber democracy: the future of democracy? *In Cyber-development, cyber-democracy and cyber-defense* (pp. 195-206). Springer, New York, NY.

Dawson, M. (2020). National Cybersecurity Education: Bridging Defense to Offense. *Land Forces Academy Review*, *25*(1), 68-75.

Dawson, M., & Omar, M. (2015). New Threats and Countermeasures in Digital Crime and Cyber Terrorism. *Hershey, PA: IGI Global*. doi:10.4018/978-1-4666-8345-7

Gikas, C. (2010). A general comparison of fisma, hipaa, iso 27000 and pci-dss standards. *Information Security Journal: A Global Perspective, 19*(3), 132-141.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems, 22*(2), 175-186.

Jaitner, M., & Mac Dermott, A. (2015, July). Cyber education? Branches of science contributing to the cyber domain. *In Proc. 14th Eur. Conf. E-Learn.* (pp. 120-128).

Kovazhenkov, M. A., Fedotova, G. V., Ilyasov, R. H., Nikitin, Y. A., & Buletova, N. E. (2019). Government control of the cyber economy based on the technologies of industry 4.0. *In The Cyber Economy* (pp. 323-333). Springer, Cham.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, *1*.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND corporation.

Libicki, M. C. (2011). Cyberwar as a confidence game. *Strategic Studies Quarterly, 5*(1), 132-147.

Mali, P., Sodhi, J. S., Singh, T., & Bansal, S. (2018). CYBER-TERRORISM AS A NON-STATE CYBER WARFARE: AN OVERVIEW. *International Journal of Civil Engineering and Technology (IJCIET), 9*(2)

Meserve, J. (2007). Mouse click could plunge city into darkness, experts say. *CNN. com*, *27*.

Moon, J., Cho, K. W., Ko, S. H., Kim, J. H., Kim, C., & Kim, Y. (2008, December). A Cyber Environment for Engineering Cyber Education. *In 2008 IEEE Fourth International Conference on eScience* (pp. 532-539). IEEE.

Nicholson, A., Janicke, H., & Watson, T. (2013, September). An initial investigation into attribution in SCADA systems. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1* (pp. 56-65).

Nye Jr, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists, 69*(5), 8-14.

Nye, Joseph. (2011). *The Future of Power.* Institute for National Strategic Security, National Defense University

Oxford English dictionary. (2013) *Oxford University Press*

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press on Demand.

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal, 12*, 21-32.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, *49*, 70-94

Saydjari, O. S. (2004). Cyber defense: art to science. *Communications of the ACM, 47*(3), 52-57.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015, September). Cyber education: a multi-level, multi-discipline approach. *In Proceedings of the 16th annual conference on information technology education* (pp. 43-47).

Syed, R., Khaver, A. A., & Yasin, M. (2019). Cyber Security: Where Does Pakistan Stand?

THINK-ASIA, Available at: https://think-asia.org/handle/11540/9714

Tehrani, P. M., Manap, N. A., & Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review, 29*(3), 207-215.

Von Clausewitz, C. (2008). *On war*. Princeton University Press.

Wong, E. (2005). Swift road for US citizen soldiers already fighting in Iraq. *New York Times, 9*.