Journal of Political Studies
Vol. 28, No. 1, January–June, Summer 2021, pp. 193–211

Foucauldian Panopticon: A Model for U.S. Cyber Surveillance

Nida Sheikh
MPhil. Scholar
Department of Political Science and International Studies,
University of Management and Technology, Lahore
Correspondence: S2019353015@umt.edu.pk

Dr. Muhammad Usman Askari
Assistant Professor
Department of Political Science and International Relations,
University of Management and Technology, Lahore.

ABSTRACT

Unlike the conventional means of surveillance in the past, cyber surveillance has become a great security tactic due to being technologically advanced, ungoverned and holistic in scope. In context of contemporary international relations, China, Russia, Iran and North Korea are using the components of information warfare to serve their strategic interests. The internationally competitive trends of information technology and surveillance make U.S. more concerned about its national security and defeating the information warfare threat. Being a global leader, U.S. is constantly developing its cyber capabilities to contain the rise of China.On account of persistent threat perception of cyber intrusions from China, U.S. has been using cyber surveillance as a counter measure. U.S has integrated its cyber capabilities with military operations in the form of aerial, land and naval surveillance to ensure its national security. The present research aims to explore that how cyber surveillance has become an indispensable component of U.S. defense strategy? Michel Foucault's surveillance theory has been used as a foundation of the study to analyze the implication of surveillance and power in context of U.S. defense policy. The study used qualitative content analysis and furthermore, directed approach has been used. The research is mainly bifold; initially it endeavors to analyze U.S. national strategies within the timeframe of 2015-2020 and subsequently discusses U.S. cyber surveillance capabilities, using the lens of Foucauldian panopticon.

Keywords: *surveillance, gaze, threat perception, power, cyber intrusions, national security, critical infrastructure*

Introduction

Likewise, the strategic significance of seas and aerospace in the past centuries, cyberspace has become a critical sphere of international relations. The present study extends the notion of Michel Foucault's surveillance theory in context of technologically advanced world where monitoring and surveillance is no more confined to spatial settings of the prison building instead it has become borderless. Surveillance lies at the core of power politics because it not merely monitors the

ongoing activities but has propensity to even predict the future actions. Foucauldian panopticon provides an architectural model that is used by U.S. in the cyber setting to meet the needs of national security. U.S. defense policies divulge that it is highly dependent on the modern-day surveillance technologies such as satellites, drones, radars, signals, scanners and numerous other means that are used for surveillance. U.S. opts the panopticon model in order to monitor military activities, armed capabilities, political strategies, corporate knowledge and other sensitive information to show preparedness against its China and other rival states.

The presently leading powerful nations maintain cyber surveillance in order to stay well prepared while keeping an eye on the activities and capabilities of enemy states. As a Prussian general and military theorist, Carl von Clausewitz said that "Knowledge must become capability." Even small numbers of forces along with the best information about the adversary's capabilities, strengths and weaknesses can defeat the large masses of enemy forces. Mongolian empire is attributed as the largest continental empire in history and they dominated on account of battlefield information. The great Mongol leader, Genghis Khan and field commanders got the information regarding the developments of battlefield no matter, even if they were thousands of miles away. Mongolian example illustrates that maintaining persistent surveillance against the emerging power of China allows U.S. to protect itself and its far-flung allies regardless of the strengths and potential capabilities of China (Arquilla & Ronfeldt, 1993). The technique of cyber surveillance has become indispensable component of U.S. national security strategy because it has been often subjected to cyber intrusions by adversary states. Numerous cyber-attacks on U.S.' critical infrastructure creates a threat perception therefore; U.S. is not merely more concerned about the cyber threats but also increasing its surveillance capabilities to ensure its defense.

Every nation has a plan to ensure its national security over the long term, keeping in view the generally uncertain as well as well-defined predetermined threats. Although there is no standard rule to draft a National Security Strategy (NSS) yet a coherent and successful strategy incorporates a brief summary of strategic vision that reflects possible future threats and specific guidelines parallel to national interests. The NSS of the U.S. aims to discuss the major security challenges and concerns of the U.S. and strategy to address them. It is a general document and its further elucidation for course of action are discussed in other relevant documents. The present study analyzed the U.S. National Security Strategy and the way it incorporates surveillance as a tactic of national security.

The first International strategy for cyberspace by U.S. government was launched in May, 2011. The integral part of the strategy emphasized on two key points; Advocating multistakeholder governance and developing norms and standards of responsible behaviour on account of states' actions. The objective behind proposing the International strategy for cyberspace was that U.S government felt insecure from cyber-attacks and presented itself to be a major sufferer and victim of cyber intrusions. The strategy accentuates international cooperation in order to secure the global internet (Zheng, 2019).

The second NSS document of U.S. was released by the Obama administration on February 6, 2015 and it emphasizes the U.S. role as a world leader. The document clearly takes a tougher line with China however, it shows desirability for

cooperation too (Lucas & McInnis, 2016).The NSS report of 2015 mentions China's rise as a major threat moreover, while discussing the strategic threats to the U.S.'critical infrastructure and cyberspace is listed at the top. Furthermore, the document states that U.S. will incorporate private sector and other stakeholders to halt any intrusion into the Federal networks.

The U.S. NSS of 2017 predicts the trajectory of great power relations. It repeatedly denounces China for using its economic and military influence to monitor the U.S. political and strategic agendas. U.S divulges its commitment to halt China from acquiring sensitive technologies that are characterized by surveillance tendencies (Tagotra, 2017). The NSS report of 2017 discusses U.S. insecurity due to growing threats in the cyberspace. It claims that state and non-state actors are involved in cyber-attacks against U.S. and cyberspace is used for modern warfare. Cyber tools are used as means to extend autocratic regimes. Furthermore, it openly claims that U.S. will deter, halt and even defeat the actors that use cyberspace against U.S. national interests.

In 2011, report of Department of Defense Cyber Strategy identifies various sources of cyber threats due to opaque architecture of the internet. It mentions multiple vulnerabilities; state and non-state actors, insiders, private groups and supply chains. Subsequently, in 2015 four countries were identified that pose major threat to U.S. in cyberspace. The report of 2015 enlisted Russia, Iran, North Korea and China. However, clear changes are notable in the report of 2018 due to more insecure cyberspace environment. The report declares that "our focus will be on the States that can pose strategic threats to U.S. prosperity and security". Moreover, this time U.S. did not identify any non-state actors and other vulnerabilities rather it enlisted the countries in a new order; China, Russia, North Korea and Iran. In the National Military Strategy of 2015 China was mentioned at fourth number. Then in 2016, China was listed second in the Defense Posture Statement and eventually, China was mentioned at the top in the National Defense Strategy of 2018 (Jinghua, 2018).

The 2015 Department of Defense (DOD) Cyber Strategy further extended the role of DOD to integrate the cyber capabilities with military operations in order to defend U.S. against the cyber-attacks. According to the new strategy, 6,200 cyber operators were categorized to ensure the protection of the department's computer networks, secure the U.S. homeland and other vital interests against any kind of cyber intrusions. Furthermore, the U.S strategy report of 2015 highlighted the attribution for deterrence and emphasized the need to collaborate with intelligence agencies and private companies. It also indicated the significance of international alliances to defend against the cyber-attacks (Zheng, 2015).

The term of "defending forward" was introduced in the 2018 report. It aimed to counter the cyber campaigns that threatened the military advantage of U.S. The active cyber defense strategy of 2011 aims to detect and mitigate threatening cyber activities and ensure to preclude malicious activities before they intrude into computer networks of DOD. In contrast to the active cyber defense, defending forward strategy of 2018 aims to stop such cyber activities at their source of origin (Chesney, 2018).

The national defense strategy and cyber strategy of U.S. in the recent five years reflect that there has been a prominent shift from traditional to non-traditional security threats. The existing hegemon is threatened due to rise of China and its use

of information warfare tactics. Last two decades are self-evident that how critical infrastructure of U.S. has been targeted by China; monitoring of sensitive information and stealing intellectual property poses a serious threat to the defense and economy of U.S. Resultantly, U.S uses the panopticon to keep an eye on its adversary as its national security is at stake. The study used Michel Foucault's theoretical lens to analyze how traditional architectural model in the shape of surveillance technology allows U.S. to exercise power against China in order to protect its national security.

Theoretical Framework

The French philosopher Michel Foucault revived Jeremy Bentham's concept of panopticon in his well-known book Discipline and Punish: The Birth of the Prison (1975). Initially, Foucault's idea of panopticon gaze was confined to a prison building characterized by asymmetrical surveillance of the prisoner: "He is seen, but he does not see; he is an object of information, never a subject in communication". Moreover, he explains the social dynamics of gaze in context of power relations. He attributed gaze as an apparatus of power relating it with surveillance. Considering the modern-day context of cyber surveillance which is accompanied with advanced network technology; the nature, form, scope and intentions of surveillance has been changed. Similarly, with the emergence of new types of surveillance, the physical structure of the panopticons has also been transformed rapidly. However, its mechanism and functionality almost remain the same. The present study used the component of power and surveillance of Foucault's model in order to analyze that how the lens of Foucauldian panopticon is used by U.S. for the purpose of national security and the way it allows U.S. to exercise power against its adversaries.

Basic Assumptions

- There is transformation in a way how power is exercised in the society
- Modern punishment has nothing to do with physical torture rather it prefers to dominate mind and soul
- Surveillance fosters relentless consciousness of being observed
- The prisoner is seen but panopticon is deliberately designed so that he cannot see
- Fear of constant observation leads to alter behaviour

Surveillance theory is basically divided into three phases however, all the phases are fiercely interlinked and interconnected in a way that dealing with any single phase in isolation would lose its real meanings and context. The study is focused on Phase I which comprises the work of Jeremy Bentham and Michel Foucault but more specifically, only Foucault's lens has been used in the present research. U.S. has been using modern technology and techniques to monitor the strategic, military, security, economic, industrial, technological, educational and other confidential activities of its adversaries. Foucault's theoretical framework appropriately elucidates the mechanism of cyber surveillance through different technologically advanced panopticons from where watching others is possible but they cannot see the observer. Nevertheless, the risk, probability and consciousness of being persistently observed or watched at any point, shapes the political behavior of states.

Research Methodology

Qualitative Content Analysis (QCA) has been used to conduct the following research. Descriptive and exploratory research approaches have been used to find out the answer of research question. As per the nature of research suggests, primary and secondary sources have been used for data collection. For data analysis, theory testing approach of QCA, Directed Content Analysis (DCA) is used. Furthermore, within DCA, manifest approach has been used.

Cyber Security as a Strand of U.S. National Security

National security is basically concerned with "who, what and where to be secured". The concept of national security is interlinked with future policy options regarding any specific national issue. After World War Two (WWII) the concept of national security became more prominent in foreign policy and international politics (Anwar, 2018).

In the twenty-first century, surveillance has become a substantial phenomenon in almost every facet of life. Surveillance by governments, military forces, corporations, law firms and foreign intelligence agencies have fostered national security concerns besides cybersecurity. The cyberspace vulnerabilities are inversely proportional to the visibility of digital intrusions; monitoring, data gathering and tracking. Cyberspace enables digital interferences which poses a serious threat to the national security. Cyber espionage and intelligence allow to collect data and information about the activities whereas electronic surveillance reveals what is said by whom, where and at what time. Hence cyber surveillance and electronic intelligence are the part of national security of every country (Banks, 2016).

In context of the present study, U.S. national security strategy of recent years declare that U.S. national security is at stake due to cyber intrusions of state as well as non-state actors. Due to persistent threat perception, U.S. uses modern surveillance technology to keep an eye on adversary and ensure its national security. U.S. has not only identified cyberspace as more sensitive domain but also endeavors to modernize its surveillance capabilities to ensure the critical infrastructure.

During the 1990s, the American, Chinese and Russian strategists proposed the functionality of networked computers and cyberspace in the context of warfare. In 2011, the Pentagon officially categorized cyberspace as the fifth domain of warfare following; land, sea, air and space as the other four important domains. The strategists assumed the phenomenon as a double-edged sword because on one side technology became an effective tool for winning the wars but on the other hand, security became vulnerable (Cavelty & Wenger, 2019).

Casting a glance at recent cyber-attacks against the United States office of personal management (OPM) in 2015, it is self-evident that the counter cyber deterrence was not only confined to China but such cyber threats also have severe implications to international cyber security. Counter cyber strategies alarmed about surveillance and suggest to use advanced cyber tools to ensure security (Putten, 2015) .

Since the foundation of People's Republic of China, the US-China relations have always been cold characterized by different conflicts and strategic mistrust. By 2015, the bilateral ties became worse and U.S. analysts suggested a dire need for a

new strategy in order to balance the emerging power of China Here a "silent contest" initiates between two great powers. Besides other major competition, cyberspace was declared as one of the most contentious areas. However, US dissatisfaction about Chinese capabilities in cyberspace is crucial in shaping U.S. national security strategy (Harold, Libicki, & Stu, 2016).

The US-led Five Eyes are cooperating to monitor and track the activities in China. According to US Defence Secretary Esper Huawei is "China's poster child for its nefarious industrial fuelled by theft and coercion and the exploitation of free-market, private companies and universities." Likewise, the Secretary of State, Mike Pompeo used the metaphor of "Trojan horse" for Chinese intelligence through Huawei. Therefore, UK might be burning bridges with U.S. if it makes any deal for launching 5th generation (5G). U.S. has clearly declared that Huawei is not merely threat to U.S. national security but to the world order (Watts, 2020).

The U.S. intelligence agencies have been reinforcing the threat of surveillance from Chinese government. They also claim that China has strategic plans to supersede U.S. economically. Chinese surveillance technology such as semiconductors, advanced quantum technology and supercomputing is used to steal intellectual and trade secrets from U.S. Using spying technology is a direct threat to the national security of United States as it would target; academia, research and development, corporate sector and above all government (Honovich, 2018).

U.S. Cyber Surveillance Capabilities

In the post-cold war era, U.S. has been attributed as the only superpower in context of military capabilities. Throwback to the Gulf war of 1991 and in 2003, the invasion of U.S. troops in Iraq demonstrates that U.S.' military superiority is fuelled by the information technology such as advanced command, control and communication system complements cyber surveillance, intelligence gathering and reconnaissance against enemy states. Although U.S. along with its allies maintain cyber surveillance to serve political, strategic and economic interests but at the same time cyberspace might prove to be U.S.' asymmetric Achilles' heel in terms of Sino-US relations. Both great powers are characterized by highly networked societies; besides, civil sector the government sector of U.S. is also vulnerable to cyber intrusions that poses severe threat to its defense and economy ending up in deteriorated bilateral ties (Spade, 2012).

U.S. has been largely developing its cyber surveillance capabilities in order to identify, monitor and track adversary's forces. ISR capabilities are fiercely integrated in military and naval missions. U.S. has highly advanced image intelligence (IMINT) mechanism to surveil on denied territories. U.S. is also highly dependent on signals intelligence (SIGINT) for monitoring at global level. Airborne surveillance capabilities have been increased in recent years to serve the U.S. national interests. E-2C aircrafts are capable of monitoring and intelligence gathering from air, land, sea and sub-surface levels (Council, 2006).

Cyber Command (USCYBERCOM) was founded in 2010 in order to protect U.S.' military assets but due to changes in the nature of cyber domain, new command vision was drafted in 2018. The command vision integrates strategic realities in order to secure and stabilize the globally interconnected digital environment (Harknett, 2018). American Marine Corps Forces Cyberspace Command

(MARFORCYBER) has freedom of action in warfighting domains therefore it integrates with other joint forces to conduct offensive cyberspace operations. Naval cyber forces of United States are integrated with Naval information forces command. It performs intelligence gathering through signals and surveillance equipment, cyber surveillance and information operations (Paul, Porche III, & Axelband, 2014). Furthermore, U.S.' alliance of five eyes pool their surveillance capabilities for mutual benefit yet it demands trade-offs in the shape of shrinking budget to develop surveillance capabilities such as aerial surveillance (Colquhoun, Knopp, & Tarapore, 2017).

U.S. uses its optical and radar sensors as a digital panopticon to constantly keep an eye on its adversaries in space. The advanced space surveillance capabilities enable US to detect and track space objects. US also identifies the source of manmade objects in the space and its anticipated timing and location to enter the earth's atmosphere. The U.S.' electro optical sensors are mainly comprised of cameras, telescopes and computers. It allows U.S. military to view real-time images of space, monitor the activities of adversary. Furthermore, the recordings can be stored to analyze later (Allahdadi, Rongier, & Wilde, 2013).

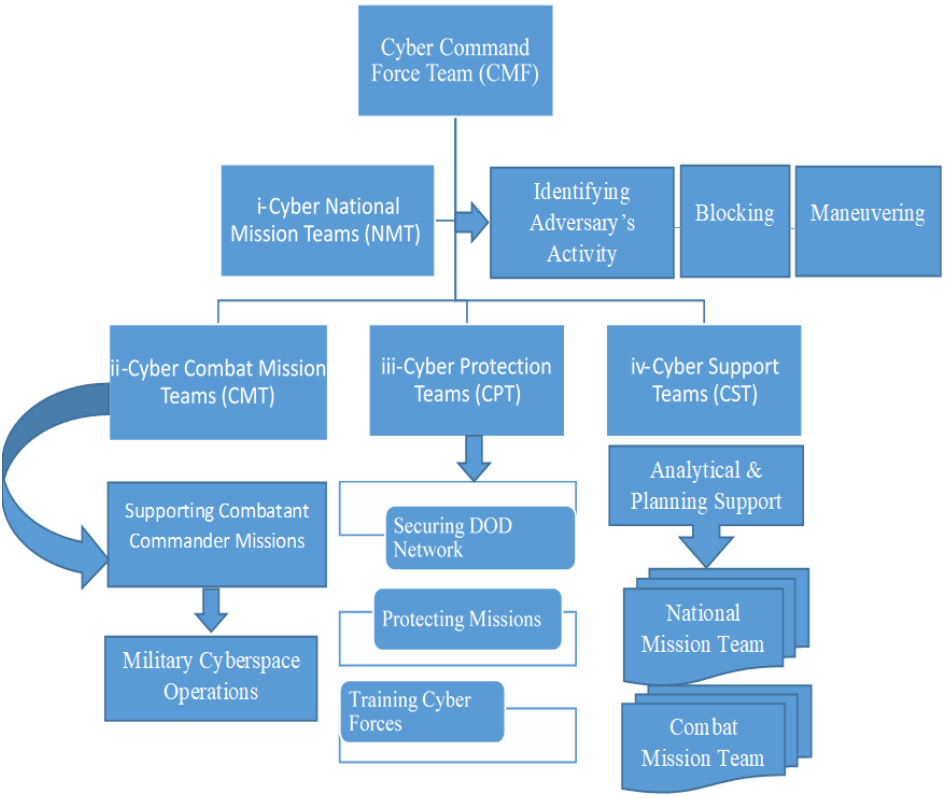
U.S.' series of satellites, known as Orion are used to scoop up microwave transmissions. Orions are capable to catch the radio signals that allow to surveil the communication of world's long-distance calls. U.S has been using these spy satellites to intercept political, strategic and economic communication from deep inside the world (Rob1blackops, 2017).

U.S. is highly dependent on cyber surveillance to advance its economic and strategic goals. The digital panopticon provides a wider window for United States into China's military capabilities, actions and intents. In 2019, ISR task force of United States shifted its focus to great power competition by identifying modernization aspects to aid cyber surveillance. A budget of $86.8 million is allocated to spark intelligence capabilities in fiscal year (FY) 2021 (Amble, 2019). The U.S. army intelligence intends to integrate with naval force for joint operations. Budget of $52 million is allocated for MDSS and developing advanced version of sensors (Army, 2020). U.S. has budgeted $22.8 million for Terrestrial Layer System (TLS) that will be used for ground-based surveillance, intelligence gathering, information warfare, cyber espionage and military intelligence.

U.S. army also aims to develop Tactical Intelligence Targeting Access Node (TITAN) for ground-based intelligence and increase military capabilities through surveillance technology. Moreover, in June 2020, National Defense Strategy Commission attributed intelligence, surveillance, and reconnaissance to be integral components of U.S military success. Referring to the increased cyber surveillance by China against U.S., it is mentioned in the congressional research report of 2020 that asymmetrical means such as cyber surveillance and other interlinked cyber capabilities are crucial to win the great power competition (Congress, 2020).

The new vision of U.S. CYBERCOM encourages to defend and maintain operational initiatives and keep the adversary disadvantaged in cyberspace. The command vision integrates strategic realities in order to secure and stabilize the

globally interconnected digital environment (Harknett, 2018).



The U.S cyber command has capability to conduct full spectrum military operations in cyberspace in order to ensure the security of DOD. Despite enjoying freedom of action in cyberspace, it denies the same access to its adversaries. Cyber command joins in NSA to maintain a dual hat relationship. In 2018, the expertise of National security agency assisted cyber command to achieve full operational capability. The cyber command force is mainly divided into four groups; each of them is assigned specific respective tasks.

i. Fully trained cyber force to ensure national security

ii. Well-equipped cyber command

iii. High ratio of qualified and certified members

iv. Capability to carry on and perform missions under stressful circumstances

v. Cyberspace operational capabilities

vi. Defending the information network of Department of defense.

vii. Skilled to provide analytical and strategic support through integrating cyber capabilities with national missions and combat missions (Command, 2018).

American Marine Corps Forces Cyberspace Command (MARFORCYBER)

The U.S. MARFORCYBER was established by U.S marine corps in January 2010. It is mainly responsible to secure the critical infrastructure of United States. The command is mainly responsible for conducting full spectrum cyberspace operations. It conducts defensive operations to secure Marine Corps Enterprise Network (MCEN). It has freedom of action in warfighting domains therefore it integrates with other joint forces to conduct offensive cyberspace operations.

MARFORCYBER is divided into three subordinate groups;

i. Marine Corps Cyber Operations Group (MCCOOG)

ii. Marine Corps Cyber Warfare Group (MCCYWG)

iii. Joint Task Force Ares (JTF) -ARES

Marine Corps Cyberspace Operations Group (MCCOG)

The major (MCCOG) responsibilities include;

i. Intelligence gathering

ii. Using cyber surveillance to develop future capabilities

iii. Identifying and reporting threats proactively

iv. Utilizing joint cyber capabilities for warfare

v. Situational awareness through surveillance

Marine Corps Cyber Warfare Group (MCCYWG)

The Marine Corps Cyber Warfare Group (MCCYWG) is responsible to perform the following tasks;

i. Administrative support

ii. Personnel management

iii. Certification (Li & Daugherty, 2015).

Sixteenth Air Force (16AF)

U.S cyber command is comprised of sixteenth air force (16AF) that plays central role in cyber surveillance. It is mainly responsible to perform the following tasks;

i. Information warfare

ii. Intelligence gathering to serve the political, economic and military interests of United States

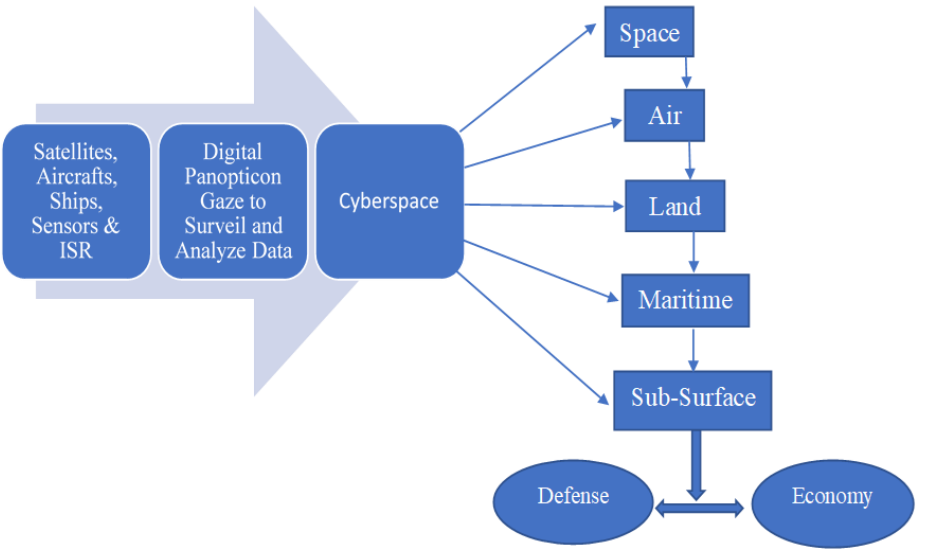
iii. Cyber surveillance

iv. Reconnaissance

v. Develop cyberwarfare capabilities (Lynch & Williams, 2009).

Despite President Donald Trump's high level of confidence in U.S' cyber capabilities to go it alone in the confrontation with China, U.S administrative members are making efforts to put together an informal coalition for intelligence

gathering against China. United States is constantly seeking for intelligence-based global partnerships to accelerate information sharing on foreign intrusions. Moreover, through such coordination United also wants to pressurize China to limit its investments in developing sensitive technologies (Barkin, 2018).



In 2019, ISR task force of United States shifted its focus to great power competition by identifying four modernization aspects to aid cyber surveillance;

i. Space
ii. Multi-Domain Sensor System (MDSS)
iii. Terrestrial Layer System (TLS)
iv. Tactical Intelligence Targeting Access Node (TITAN)

The first modernization initiative aims to upgrade space-based surveillance through signals intelligence to keep an eye on the activities of adversaries.

U.S. aims to develop the capabilities of Army Intelligence and Security Command through introducing Multidomain Sensor System (MDSS). It is characterized by following features;

i. Operates at medium as well as high altitudes
ii. Geospatial coverage with sensing
iii. Full motion video coverage
iv. Intelligence sensors
v. Identifying targets
vi. Long range precision targeting

Sensors enabled with artificial intelligence serves as synergy in identifying the enemy and immediate targeting.

A Glance over the Last Two Decades: Major Cyber Surveillance Campaigns of United States and China

Throwback to last two decades show that US and China have been persistently monitoring and attacking on the critical infrastructure of each other. Tabular representation of major surveillance campaigns is given below;

TITAN RAIN (2003-2006)	A string of cyber surveillance operations by China to monitor the military capabilities and other sensitive institutions of United States
SHADY RAT (2006-2010)	Cyber surveillance by China against U.S government and many other countries
GHOSTNET (2007-2009)	Political, economic and media institutions of approximately more than hundred countries were targeted by China
HIKIT (2008-2014)	Worldwide cyber surveillance by China to monitor the data and collect information from media houses, IT firms, educational institutions and government offices
BYZANTINE SERIES (2008-2011)	China initiated cyber surveillance to keep an eye on U.S institutions
NIGHT DRAGONS (2009-2011)	Cyber surveillance by China to spy on critical infrastructure of United States
OPERATION AURORA (2009-2010)	Cyber surveillance by China against U.S IT firms such as Google, Apple and others
OPERATION SHOTGIANT (2010-2014)	It was initiated by United States to keep an eye on the activities of Huawei
OPERATION BEEBUS (2011-2013	China's cyber surveillance to monitor the U.S Department of Defense

OPERATION IRON TIGER (2013-2015)	Asian and US-based telecommunication industries, IT firms and energy companies were targeted by China
(2014– 2015)	China has been involved in the data breach of US Office of Personnel Management

Since the mid-1950s, Sino-Russian alliance has been strengthening and in coming years their bilateral relation will improve due to mutual interests. Both countries have a common adversary and their threat perception is shaped by unilateralism, interventionist policies and spread of democratic values by the United States. Likewise, the expanding regional and global influence of China and Russia, U.S allies are endeavouring to persuade Washington for greater independence. In response, U.S has become more open to bilateral and multilateral partnerships on security and trade in order to contain the emerging power of China. U.S. claims that besides Russia, Iran and North Korea, China poses a constant threat to U.S. intellectual property and critical infrastructure through cyber surveillance. In addition to that, U.S. attributes China to be the strongest strategic competitor that has been involved in monitoring the sensitive information of U.S. government offices, industries, technology sectors and allies. United States claims that U.S. cyber capabilities are necessary to defend its critical infrastructure against Chinese intelligence and information technology (Coats, 2019).

In 2013, the U.S. Director of National Intelligence, James Clapper said that cyber security is the major security threat to the United States. Besides rapid expansion of internet technology, artificial intelligence and internet of things will contribute to increase the number of internet connections up to trillions in the coming decade. Increased network connectivity will also expand he cyber surface vulnerable to cyber intrusions. Cyber behaviour is no different than other social behaviours such as crime therefore, many governments incorporate the idea of Robert Jervis' deterrence in the cyber era. Due to increased cyber surveillance of China, U.S. government has asserted to implement laws of armed conflicts in cyberspace too (Nye, 2018).

In July 2018, the US-China trade war initiated as United States Trade Representative (USTR), imposed tariffs on Chinese products due to intellectual property theft. U.S imposed high tariffs and trade barriers on technological sectors and products such as; aerospace, telecommunication, IT, robotics, computing and other important machineries, semiconductors and batteries. The major issue repeatedly highlighted by the Trump administration was that China has been stealing U.S trade secrets to forcefully transfer U.S technology through unfair trade practices which is a direct threat to U.S national security.

The trade war has contributed to tit-for-tat trade barriers and sanctions against each other. Beside technology sector, trade war has also affected other manufacturing sectors. Furthermore, deteriorated bilateral ties also warned the companies of cyber intrusions along with imposition of new policy regulation (Mikhail, 2018).

U.S claims that technology giants in China are hardly subjected to strict regulations or due to having close ties with military their surveillance practices expand to critical

infrastructure (Aho, 2020). In December 2020, United States backlisted Semiconductor Manufacturing International (SMIC) and Shenzhen Da-Jiang Innovations (SZ DJI). The major allegation on SMIC was that it maintains close ties with military industrial companies of China. Dozens of other Chinese firms were blacklisted by U.S due to their affiliation with Chinese military and serving other national interests through stealing trade secrets and monitoring private information. SZ DJI Technology Co is accused that its drone machinery has capability of cyber-enabled surveillance as it has tendency to transfer sensitive information to China. Prior to that Huawei along with its 150 affiliated firms were blacklisted due to cyber espionage and cyber intrusions into U.S companies (Pamuk, Shepardson, & Alper, 2020).

On December 21st, 2018 Australia joined Britain, New Zealand and United States to initiate a global campaign against intellectual property theft. The purpose of campaign was to increase global coordination against China's cyber surveillance that enables to steal commercial-based intellectual property. The APT10 from China was alleged of various cyber intrusions at global level. Furthermore, Chinese intellectual property theft was condemned as it just not poses a national security threat but also undermines the global economic growth (Australia, 2018).

Additionally, U.S. also presents the analogy of cyber pearl harbour. The contemporary cyber domain has destructive tendencies that is threatening to the national and economic security of the United States. It elucidates that China along with its allies maintains surveillance to monitor the vulnerabilities of U.S Cyberspace and get access to its control points. It predicts that in case China launch a cyber-pearl harbour against U.S then it is more likely to target the U.S institutions that are critical to U.S economy such as; electronic voting systems. Power grids, undersea cables, banking systems and other infrastructure crucial to internet commerce (Perkovich & Levite, 2017).

Discussion and Results

U.S. is the existing hegemon whereas rise of China poses threat to the global leadership, dominant role of U.S in international world politics and unipolar world order. Besides contentious relations in other spheres, cyberspace has become a new battlefield for the great powers. Instead of conventional military power, U.S. is more focused on constantly increasing its cyber capabilities due to security dilemma. In fact, integration of cyber power with military operations become a synergy. Rise of China is not only a threat to U.S.' global leadership but also to its national security as U.S.'critical infrastructure is vulnerable to cyber intrusions by China. Therefore, U.S. is making increased investments in R&D, innovation and surveillance technology. These surveillance technologies serve as a panopticon to keep an eye on adversary and convert that information into capabilities. U.S. is using surveillance to stay proactive and vigilant against China and such means of hidden surveillance make it powerful and dominant. According to Foucault, the gaze of the watcher is inevitably internalized in a way that there is no need of any external actions. Surveillance allows U.S. to keep an eye on its adversaries and show preparedness accordingly i any direct confrontation in the battlefields.

The validity of the metaphor of "panopticon" has not become obsolete even to this day as the mechanism of "watching and being watched" is carried out through modern technologies. Foucault protracted his ideas in context of power relations and

networks in the modern age. Foucault demonstrated that besides prison, architecture of panopticon is applicable for other sections of the society, specifically while exercising power relations in governance. Technological advancement has transformed the conventional surveillance practices. Michel Foucault's notion of surveillance is no more confined to spatial settings of prison rather it has been extended to organizational and state level practices. In today's world, conduct of warfare has been altered from battle fields to cyberspace. Unlike historical wars, in coming future, world is more likely to experience cyber warfare and information warfare. Consequently, cyber surveillance has become an important aspect of international relations. Foucault claims that surveillance is characterized by domination, power and control. The authenticity and relevance of Michel Foucault's theory in the present-day world can be elucidated with the following statement of David Lyon "we cannot evade some interaction with the Panopticon, either historically, or in today's analyses of surveillance". U.S. has fiercely integrated cyber capabilities with military operations that serves as synergy. Victory is no more determined by number of soldiers rather it is dependent on informationalization; how much you know about the strengths and weaknesses of your adversary. Digital panopticon is used by U.S. to monitor the activities of adversaries and show preparedness accordingly. Modern day surveillance has no limited objectives of behavioural correction and work efficiency rather states use surveillance to monitor their adversary.

Findings

- The contemporary cyber domain has destructive tendencies that is threatening to the national and economic security of the United States
- Components of Foucault's panopticon model; power and surveillance are applicable in context of U.S. surveillance capabilities against China however, its means, intensity and objectives are relatively different.
- In the modern technological world, surveillance poses a national security threat to states and at the same time it is used by great powers to advance their national interests and ensure national security.
- U.S. has been increasing its cyber capabilities on account of its cyber security and national security.
- Although U.S has been historically involved in cyber surveillance but it began to rely more on surveillance specifically, after the event of 9/11.
- In 2019, ISR task force of U.S. shifted its focus to great power competition through cyber surveillance
- U.S use signals intelligence and ISR capabilities to monitor the military and naval activities of adversary states in the South China Sea. Besides that, five eyes alliance also gather intelligence that is used to serve U.S. national interests.

Conclusion

Foucault's notion of surveillance in a prison building endorsed that power relations are created irrespective of the watcher, is applicable at macro level cyber surveillance of U.S. as most of the times either surveillance could not be detected or watcher remains anonymous. However, there is constant fear, risk and insecurity of

being surveilled through cyber intrusions therefore, U.S uses the model of panopticon to stay vigilant against its adversaries. Doubtlessly, in context of U.S. cyber surveillance through digital panopticon serves as a window to peek outside and stay updated by keeping an eye on adversary. Michel Foucault's concept of surveillance mainly characterized by domination, power and control could be envisaged as happening in its entirety, using the new digital panopticon which, in contemporary technological world has no limitation, no borderlines and even no visible legislations on account of cyber surveillance.

Recommendations

- United States should negotiate with China over accelerating cyber surveillance and the way it is threatening to the U.S. economy and defense. It is important to define cyberspace rules without leaving any room that could be problematic or contentious in future. Although both countries have already signed agreement, defense strategies have been drafted and above all cyber security laws are there yet there is dire need to narrow down them. For Example; The 2016 "Directive on security of network and information systems" (NIS Directive) of EU is scrupulous example of comprehensive legislation that encompasses all aspects of cyber security.

- The leading great powers should identify the extensive implications of cyberspace tussle as it is a high time to realize that how the negative use of digital panopticon against each other has affected the broader health of Sino-US relations. i.e., In context of EU all member states agreed to cooperate due to mutual strategic interests. Cyber security cooperation would strengthen economic and diplomatic ties as numerous sectors; defense, energy, water, banking, health care, research centres, universities and national security are subjected to cyber threats.

- Deterrence could also be helpful in the following context by defining strict rules and proper legislation against cyber intrusions, cyber surveillance and espionage. Being leading world powers, increased interdependence of networks itself creates deterrence. U.S. have sufficient resources to invest in cyber security programs at international level.

- In order to mitigate the mistrust due to numerous past incidents of cyber surveillance, evidentiary standards could be set out. China should cooperate with U.S. for sake of revitalizing the trust factor and clarify its position by rationally elucidating that what has actually been done.

- United States and China need to reconsider their protectionist policies against the foreign tech giants. Throwback to 2010 and 2014, divulges that U.S.' scaling back economic sanctions and plans of reopening the embassies contributed to strengthen diplomatic ties with Cuba. In context of Sino-US relations, US should play its role as a global leader to strengthen the diplomatic and economic ties with China.

References

[1] Ackerly, B. A., Stern, M., & True, J. (Eds.). (2006). *Feminist methodologies for international relations*. Cambridge, England; New York: Cambridge University Press.

[2] Becker, H. S. (1967). Whose side are we on?. *Social problems*, *14*(3), 239-247.

[3] Bryman, A. (2008). *Social research methods*. Oxford university press.

[4] Corbin, J., M. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Los Angeles, Calif; London: Sage Publications, Inc.

[5] Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. London: Sage.

[6] Denzin, N. K., & Lincoln, Y. S. (2008). *Strategies of qualitative inquiry* (Vol. 2). Los Angeles: Sage Publications.

[7] Guba, E. G., & Lincoln, Y. S. (1998). Competing paradigms in qualitative research. in N.K. Denzin& Y.S. Lincoln (Eds.), *The landscape of qualitative research.* (pp.?-?). Thousand Oaks, CA: Sage.

[8] Hammersley, M. (2001). Which side was Becker on? Questioning political and epistemological radicalism. *Qualitative Research*, *1*(1), 91-110.

[9] King, G. (1994). *Designing social inquiry: Scientific inference in qualitative research*. Princeton, N.J. Chichester : Princeton University Press.

[10] Lynch, M. (2000). Against reflexivity as an academic virtue and source of privileged knowledge. *Theory, Culture & Society*, *17*(3), 26-54.

[11] Matthews, B., & Ross, L. (2010). *Research methods*: *A practical guide for the social sciences.* Pearson.

[12] Ramazanoglu, C. (2002). *Feminist methodology: Challenges and choices*. London: Sage.

[13] Rubin, H. J. (2005). *Qualitative interviewing: The art of hearing data*. Thousand Oaks, 2nd Edition, Calif; London: Sage Publications.

[14] Welland, T., & Pugsley, L. (2002). *Ethical dilemmas in qualitative research*. Aldershot: Ashgate. Aho, B. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 3-5. doi:10.1080/03085147.2019.1690275

[15] Allahdadi, F. A., Rongier, I., & Wilde, P. D. (2013). *Safety Design for Space Operations.* Noordwijk: International Association for the Advancement of Space Safety.

[16] Amble, J. (2019). *MWI Podcast: intelligence and the future battlefield, with lt. gen. scott berrier.* New York: Modern War Institute.

[17] Anwar, M. A. (2018). Mapping the knowledge of national security in 21st century a bibliometric study. *Cogent Social Sciences*, 1-5. doi:https://doi.org/10.1080/23311886.2018.1542944

[18] Army. (2020). *Department of Defense Fiscal Year (FY) 2021 Budget Estimates.* Washington D.C: Department of Defense.

[19] Allahdadi, F. A., Rongier, I., & Wilde, P. D. (2013). *Safety Design for Space Operations.* Noordwijk: International Association for the Advancement of Space Safety.

[20] Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is Coming!* Santa Monica: RAND.

[21] Australia, P. o. (2018). *Attribution of Chinese cyber-enabled commercial intellectual property theft.* Canberra: Parliment of Australia.

[22] Banks, W. C. (2016). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Law Journal*, 514-524.

[23] Barkin, N. (2018). *Exclusive: Five Eyes intelligence alliance builds coalition to counter China.* Toronto: Thomson Reuters Corporation.

[24] Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 5-32. doi:10.1080/13523260.2019.1678855

[25] Chesney, R. (2018). *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes.* Washington, D.C.: LAWFARE.

[26] Coats, D. R. (2019). *worldwide threat assessment of the us intelligence community.* Washington, D.C.: United States Senate Select Committee on Intelligence.

[27] Command, U. C. (2018). *Cyber Mission Force achieves Full Operational Capability.* Maryland: U.S. Cyber Command Public Affairs.

[28] Congress, C. o. (2020). *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition.* Washington D.C: Congressional Research Service.

[29] Council, N. R. (2006). *C4ISR for Future Naval Strike Groups.* Washington, D.C.: The National Academies Press. doi:https://doi.org/10.17226/11605

[30] Colquhoun, C., Knopp, B., & Tarapore, A. (2017). *Five Eyes at 70: Where to from Here?* Santa Monica: RAND.

[31] Harknett, R. J. (2018). *United States Cyber Command's New Vision: What It Entails and Why It Matters.* Washington, D.C: LAWFARE.

[32] Harold, S. W., Libicki, M. C., & Stu, A. (2016). *Getting to Yes with China in Cyberspace.* Santa Monica: RAND Corporation. doi:10.7249/rr1335

[33] Honovich, J. (2018, September 7). *China "Largest Threat To US National Security", Declares FBI And Counterintelligence Heads*. Retrieved from IPVM: https://ipvm.com/reports/china-evanina

[34] Jinghua, L. (2018). *A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward'.* Washington, D.C: Carnegie Endowment for International Peace.

[35] Libicki, M. C. (2017). The Convergence of Information Warfare. *Strategic Studies Quarterly*, 1-2.

[36] Li, J. J., & Daugherty, L. (2015). *Training Cyber Warriors What Can Be Learned from Defense Language Training?* Santa Monica: RAND.

[37] Lucas, N. J., & McInnis, K. J. (2016). *The 2015 National Security Strategy:*.Washington, D.C: Congressional Research Service.

[38] Lynch, K. F., & Williams, W. A. (2009). *Combat Support Execution An Assessment of Initial.* Santa Monica: RAND.

[39] Mikhail, G. (2018). *Boom, How the US and China Trade War Caused Cybersecurity.* Singapore: Datasearch Consulting.

[40] Nye, J. S. (2018, February). *Preventing a cyber-Pearl Harbor is not the only digital challenge nation states face*. Retrieved from The Security Times: https://www.the-security-times.com/preventing-a-cyber-pearl-harbor-is-not-the-only-digital-challenge-nation-states-face/

[41] Pamuk, H., Shepardson, D., & Alper, A. (2020). *U.S. blacklists dozens of Chinese firms including SMIC, DJI.* Totonto: Reuters.

[42] Paul, C., Porche III, I. R., & Axelband, E. (2014). *The Other Quiet Professionals Lessons for Future Cyber Forces from the Evolution of Special Forces.* Santa Monica: RAND.

[43] Perkovich, G., & Levite, A. E. (2017). *Why a Digital Pearl Harbor Makes Sense . . . and Is Possible.* Washington, D.C.: Georgetown University Press.

[44] Rob1blackops. (2017, September 24). *A radiotelescope in the sky: the USA-202 ORION satellite*. Retrieved from SatelliteObservation.net: https://satelliteobservation.net/author/rob1blackops/

[45] Spade, J. M. (2012). *'China's Cyber Power and America's National Security'*. Carlisle: Army War College (U.S.).

[46] Tagotra, N. (2017). *The US National Security Strategy and Great Power Relations.* Washington D.C: The Diplomat.

[47] Watts, G. (2020, February 22). *China takes a stab at one of the 'Five Eyes'*. Retrieved from ASIA TIMES: https://asiatimes.com/2020/02/china-takes-a-stab-at-one-of-the-five-eyes/

[48] Zheng, D. E. (2015). *2015 DOD Cyber Strategy.* Waswhington D.C: Center for Strategic and International Studies.

[49] Zheng, L. (2019, July 5). *Security*. Retrieved from China US Focus: https://www.chinausfocus.com/peace-security/us-cyber-attacks-on-iran-may-change-the-rules-of-war