Collabits Journal
Vol. 1 No. 3 September 2024 : 119-128
E-ISSN : 3046-6709, P-ISSN : 3062-8601
https://publikasi.mercubuana.ac.id/index.php/collabits

The Role And Evolution Of Computer Technology In Military Strategy: A Perspective From The World War II Era To The Contemporary Cyber Warfare Era

Siti Maesaroh[1], Nathanael Aurick Adventius Putra Hermawan[2], Syilmi Isneni[3*]

[1,2,3] Computer Science study program, Universitas Mercu Buana, Jakarta, Indonesia

*Coressponden Author: syilmiisneni03@gmail.com

Abstract - Computer technology has become a crucial element in military strategy from the World War II era to the contemporary Cyber War era. During World War II, early computers were used to crack enemy encryption codes and optimize the trajectories of artillery projectiles. As development progressed, electronic computers emerged, providing faster and greater computing capabilities. In the Cold War era, computers were used in war simulations and the development of missile defense systems. Then, with the advent of the Cyber War era, computer technology became central to military operations, used in cyber monitoring and defense, intelligence analysis, and network operations. The transformation of computer technology from mainframe computers to global networks has changed the landscape of modern warfare, enabling the development of sophisticated cyber weapons and tactics. In this context, this article reviews the use and transformation of computer technology in military strategy from World War II to contemporary Cyber Warfare, highlighting the key role of computers in shaping the dynamics of modern warfare.

Keywords :

WWII;
Cold War;
Gulf War;
Cyber War;
Technology;

Article History:
Received: 10-07-2024
Revised: 24-08-2024
Accepted: 15-09-2024

Article DOI : 10.22441/collabits.v1i3.27315

1. INTRODUCTION

Since World War II, computer technology has been a crucial element in military strategy, undergoing significant evolution until the contemporary era. Initially used to break enemy secret codes and improve artillery accuracy, the role of computers has continued to evolve over time. The advent of electronic computers provided greater computing power, enabling use in war simulations and the development of missile defense systems during the Cold War. However, the most striking change came with the advent of Cyber Warfare, where computer technology became the core of military operations. From cyber monitoring and defense to intelligence analysis and complex network operations, computers have fundamentally changed the landscape of modern warfare. With the transition from mainframe computers to global networks, sophisticated cyber weapons and tactics became possible. Understanding the key role of computer technology in shaping the dynamics of modern warfare is crucial, as it has influenced military strategy, tactics and operations across the board.

2. RESEARCH METHODOLOGY

The methodology used was historical and descriptive analysis. The research involved collecting historical data on the use of computer technology in military contexts from World War II to the contemporary Cyber Warfare era. It also conducted a detailed analysis of how the evolution of computer technology influenced military strategy during this period. The methodology involves literature searches, case studies, as well as interviews with military experts or practitioners to gain deeper insights into the impact of computer technology in military strategy Discussion.

3. RESULTS AND DISCUSSION

3.1 World War II and the Early Use of Computers

World War II occurred in 1939, a military conflict that covered almost all countries in the world at that time. This conflict is a continuation of the previous conflict, namely the first world war. Some of the determining factors in the occurrence of the Second World War included the peace agreement at the end of the First World War (Versailles), which was more profitable for the alliance, resulting in dissatisfaction from the losing party. Like Germany which lost 13% of its territory to give to France as war booty, reducing the number of military forces, especially the German air force . There is an economic and social crisis which results in economic instability, mass unemployment and social tension. High levels of nationalism and political extremism. The existence of Imperialism's ambition to expand territory

and the failure of the League of Nations to guarantee world peace at that time also became a factor in world war that could occur again.

World War II began with the German invasion of Poland in September 1939 and ended in 1945 when Japan surrendered unconditionally to the Allies. This global conflict, which has claimed more than 55 million human lives, provides a stage and opportunity for the combination of military power and technology to become one unit for a goal to be achieved. World War II also proved the basic nature of humans which is not far from violence and oppression of fellow humans who are considered inferior or weak, the emergence of racism, excessive exploitation of resources, using all means without prioritizing humans, nations or other groups to achieve a goal. own nation or group.

World War II also proved the effectiveness of combining military power with existing technological advances, which could determine the direction of the war. During war, a lot of technology was used to maximize the possibility of victory in a battle, until the era of using the first generation of computer machines in the world began. It cannot be denied that with the events of World War II the progress and development of computer technology developed very rapidly, at that time there were many names of great scientists who became pioneers in the development of computer technology, such as John William Mauchly and J. Presper Eckert who discovered ENIAC, Tommy Flowers who invented the Colossus engine and many more.

3.1.1 COLOSSUS

During World War II, encryption played a crucial role in securing battlefield communications, with both Allied and Axis powers developing machines to decipher encrypted messages. Germany utilized two main military transmission methods: Enigma, which broadcast in Morse code, and "Fish" or "Tunny," transmitted in binary code.

Tunny, used for encrypting high-level messages from Hitler to the German military command, operated with a teleprinter, converting each letter into a 5-bit teleprinter code, akin to modern computer keyboard conversions to binary. The encrypted messages were then obfuscated by the Tunny machine, producing seemingly random jumbles of letters. In 1942, Bletchley Park coder William Tutte discerned a systematic pattern in Tunny messages.

Before the development of Colossus, the "Heath Robinson" analytical machine utilized photoelectric technology to read two punched paper tapes concurrently, but it proved slow and unreliable. Engineer Tommy Flowers conceived Colossus, a faster and more reliable analytical machine, primarily designed for double-delta attacks against Lorenz ciphers but adaptable for Tunny decryption. Colossus read paper tape at 5,000 characters per second, significantly faster than Heath Robinson.

Driven by a tape reader, Colossus scanned punch holes in a tape representing the cipher text, converting them into pulses for processing by its arithmetic and logic circuits. The machine employed a delta circuit to calculate the differences between consecutive bits, with a counter tracking instances where combinations of delta streams produced zero.

To enhance computing speed, Colossus utilized a shift register to store the last six bits of tape, enabling five comparisons in parallel. This innovation allowed for five times more German messages to be processed simultaneously.

After the war, Colossus was destroyed, and all related plans and information were burned to maintain secrecy.

3.1.2 ENIAC

ENIAC is a computer The first general-purpose programmable electronic digital device created by the United States during World War II. American physicist John Mauchly, American engineer J. Presper Eckert Jr. and colleagues at the Moore School of Electrical Engineering in Pennsylvania began a government-sponsored project to build an electronic computer.

ENIAC work began in early 1943.The ENIAC was specifically designed to calculate artillery array values, this machine lacks some features that would make it more generally useful. It transmits instructions to the machine through a pin board; the advantage is that once the instructions are "programmed" the machine runs at electronic speed. Instructions read by a card reader or other slow mechanical device would have been no match for the all-electronic ENIAC. The downside is that it can take days to assemble a machine for each new problem. It is a responsibility that can only be called programmable with a little generosity (Sudirman & Wahono , 2003).

However, ENIAC was by far the most powerful computing device ever created. It is a digital computer, the first general purpose programmable electronics. Like Charles Babbage's Analytical Engine (from the 19th century) and the British World War II Colossus computers, it had conditional branching, ie. different instructions could be carried out or change the order in which the instructions were carried out. value of some data. (For example, the IF ENIAC was very large.

The ENIAC lived in a 50-by-30-foot (15 by 9-meter) basement at the Moore School, where its 40 panels were arranged in a U-shape along three walls. Each panel is approximately 2 feet wide, 2 feet deep and 8 feet long (0.6 meters x 0.6 meters x 2.4 meters). With more than 17,000 vacuum tubes, 70,000 resistors, 10,000 capacitors, 6,000 switches and 1,500 relays, it is the most complex electronic system ever created. The ENIAC ran continuously (partly to extend the life of the tubes), produced 174 kilowatts of heat, and thus needed its own air conditioner. It can perform up to 5,000 additions per second, several times faster than its electromechanical predecessor. These and later computers that used vacuum tubes are known as first-generation computers. (Thanks to the 1,500 mechanical relays, the ENIAC was still in the transition to a fully electronic computer.) (Swaine, Michael, & Paul, 2024).

The ENIAC used a ring counter with ten positions. Counting is done by "counting" pulses with a ring counter

and generating a new carrier pulse when the counter is wound back to its original position; the main idea was to imitate a number wheel in a mechanical calculator. The

ENIAC had twenty battery slots, each holding ten digits, and every second it could do 5,000 simple additions and subtractions between those twenty digits. Four battery slots are used with the "flat" and any other 385 multiplication process can be done. 5 battery slots controlled by a "square root divider" can do 40 division operations and 3 square root operations per second. The other nine devices are the "start unit" (start and stop the machine), the "bike node" (synchronize other devices), the master programmer (controls the circuit sequence), the read unit (controls the IBM punch card reader), the standard transmitter, and three function tables.

The ENIAC uses a doctal-based radio tube, which was commonly used at the time, the decimal module was made from a 6SN7 flip-flop, while the logic functions use a 6L7, 6SJ7, 6SA7 and 6AC7. A large number of 6L6 and 6V6 devices are used as "line drivers" to drive pulses between control frame cables. Completed in February 1946, ENIAC cost the government $400,000 and the war ENIAC was supposed to have won was over. His first task was to make calculations for the production of a hydrogen bomb. Some of these machines are on display at the Smithsonian Institution in Washington.

ENIAC was in operation until October 21, 1955. The design was never replicated and as a result its bugs, most notably the inability to save programs, were never fixed. But the ideas of the work and its influence on people like John von Neumann loom large in the development of the next generation of computers, originally EDVAC, EDSAC and SEAC. There have also been several improvements to the ENIAC since 1948, including a read-only stored programming mechanism. Archived 2010-01-03 at the Wayback Machine. which uses a function table as a ROM program was proposed by John von Neumann. This change reduced the speed of the ENIAC by a factor of 6, but also reduced the programming time to hours (from earlier days), so that the loss of speed was considered acceptable. Until 2004, the 0.5 mm square a chip silicone is the same as ENIAC, which occupied one underground chamber (wikipedia, 2024)1947.

3.1.3 EFFECT ON WAR

The use of computers in the Second World War had a huge effect on the course of the war. Especially the use of computers as imaging machines or secret code breakers that really helped the allies determine the right military strategy. The success of the Colossus machine in breaking the Tunny and Enigma codes influenced many military operations, such as the breaking of the Enigma code, which drastically reduced the number of German submarines in the Atlantic, the largest of which were the Allied landings on the coast. Normandy in June 1944 (Copeland, 2024). The use of calculators on the German side Electronics such as the Zuse Z3 aided artillery planning calculations and logistical planning, allowing the Germans to increase the accuracy of artillery strikes and manage logistics effectively. There are several other technologies that were precursors to the technologies we use today, such as the early analog machines used to control the V-2 rocket for trajectory and navigation calculations that became the basis for modern rocket production, and many other technologies. like radar. which is still used today.

3.2 The Cold War and The Technological Race

The destruction of the Japanese cities of Hiroshima and Nagasaki by American atomic weapons in August 1945 sparked the start of an arms race between the United States and the Soviet Union. This not only caused unimaginable harm to the Japanese population, but also had a profound impact on a generation that grew up under the shadow of the threat of nuclear holocaust. The success of the atomic bomb in World War II not only marked a new peak of power in the history of warfare, but also encouraged both superpowers to develop their own atomic technology to maintain their status (swift , 2009).

The Cold War, which occurred between 1947 and 1991, set the stage for ideological competition between liberalism led by the United States and communism supported by the Soviet Union. This period was marked by the formation of defense alliances such as NATO and the Warsaw Pact, as well as a series of interventions in various countries to expand the ideological influence of each bloc. In the midst of technological races such as the Space Race, tensions between the United States and the Soviet Union created a time of global uncertainty and instability (hapsari & adil, 2018).

Fears of human extinction are increasing with the frightening accumulation of nuclear weapons, which exceeds any goal in terms of national security. This arms race not only creates physical threats, but also presents ongoing psychological threats, with widespread concern that a single mistake or misunderstanding could trigger mass destruction. Thus, the Cold War era reflected deep anxiety about the possible extinction of humanity due to the impact of uncontrolled political and military tensions After the Second World War, the US Navy and US Air Force noticed difficulties in air defense battle management, especially during Japanese kamikaze air raids. They realized that air defense in the jet age required automation. The Navy developed the Naval Tactical Data System (NTDS), while the Air Force created the Semi-Automated Ground Environment (SAGE). Both systems integrate computer technology to improve battle management.

Collaboration between the military, industry, and academia resulted in technological advances such as transistors, integrated circuits, and the Univac computer. The Department of Defense created the Advanced Research Projects Agency (ARPA) to explore computer internet technology, which became a major focus in 1959. The Cuban missile crisis of 1962 highlighted the importance of data sharing across military command and control systems. Efforts to consolidate command and control systems resulted in the Worldwide Military Command and Control System (WWMCCS).

The computer industry in the West took the lead in producing smaller, more powerful, and more connected computers in the 1970s, 80s, and 90s, in accordance with Moore's law proposed by Gordon E. Moore in 1965. On the Block Soviet, the computer industry experienced difficulties and lagged behind in technological development.

On the Soviet side Cybernetic theory in the post-World War II era was met with incomprehension and suspicion among Soviet Party leaders, who condemned it as a capitalist plot. However, the need for computers was recognized by Soviet military and economic planners, leading to the dilemma alluded to by Ogarkov in 1983.

After Stalin's death in 1953, cybernetics slowly began to regain its footing in Russian academic and industrial institutions. Khrushchev, in an effort to liberalize and reform the economy, introduced de-Stalinization policies and decentralized economic management. However, this decentralization also brings challenges, as Ogarkov highlights (leese, 2023).

Although Khrushchev's new policies initially succeeded in boosting the Soviet economy and arms sales, optimism about the possibility of defeating capitalism faded. Further decentralization is needed, but regional sub-committees need access to production data and economic planning, which requires the use of cybernetics and computers.

However, extensive administrative decentralization backfired on the Soviet system. Internal strife and an inability to collaborate limited cybernetic reform efforts. The Soviet military used computers to improve warning strategies, but efforts such as ARPANET proposed by Kitov were rejected and he was even removed from office.

While the Soviet military focused on highly classified cybernetic efforts, civilian efforts lagged, and a lack of inter-organizational coordination hampered the practical development of cybernetic theory in the Soviet Union, especially compared to the West

US-Soviet tensions peaked in 1983 due to several key events. On March 8, Ronald Reagan called the Soviet Union "the focus of evil in the modern world" and supported the development of a Strategic Defense Initiative (SDI) against ballistic missiles. This announcement caused tensions to rise, especially after incidents such as the shooting down of Korean Airlines flight 007 by the Soviets and the US invasion of Grenada.

SDI, known as the "Star Wars" program, aimed to render Soviet ballistic missiles defenseless. Although many doubted its feasibility, Reagan succeeded in forcing the Soviets to reevaluate their strategy. The CIA exploited Soviet reliance on industrial espionage by providing false information regarding advances in US laser technology.

Economic pressure on the Soviets increased as they were already spending 10-15% of GNP on the military and facing a costly war in Afghanistan. Reagan's doctrine, which included SDI, economic sanctions, and coercive diplomacy, further worsened the Soviet situation. Reagan's strategy succeeded in creating a perception of US technological superiority and sowing uncertainty in Soviet military planning, ultimately forcing them to attempt to normalize relations with the US.

3.2.1 SAGE

In 1949, President Harry Truman announced that the Soviet Union had succeeded in developing its own nuclear bomb, and no less surprisingly, the Soviet Union had succeeded in developing a long-range aircraft capable of delivering nuclear bombs to America. arctic road This statement made the Americans nervous, because the GCI (Ground Control of Intercept) radar defense system developed at the time during World War II was designed only for conventional weapons and had limitations in detecting incoming enemy aircraft. These concerns led to the creation of the Valley Committee, which was tasked with analyzing air defenses in anticipation of Soviet air attacks. After analysis, the commission concluded that the weakest link in air defense is the radar, which should be able to detect low-flying aircraft.

The commission continued to analyze the issue and narrowed it down to two main issues. First, to interpret the signals from multiple probes, it must be possible to send the radar data to a central computer where it can be compiled. Second, since the goal is to detect and intercept enemy aircraft, computers must analyze the data in real time. The scope of the SAGE air defense system from its inception in 1951 to its full deployment in 1963 was enormous. The cost of the project, both in terms of funding and the number of military, civilian and contractor personnel involved, exceeded the cost of the Manhattan Project (an atomic bomb project). The project name evolved over time from the Lincoln Project, originally named in 1951, to the Lincoln Transition System, and finally to the Semi-Automatic Field Environment, or SAGE. Briefly, the basic SAGE architecture consists of: (1) a radar network and other data sources, and (2) a digital computer that (a) receives radar and other data for aircraft detection and tracking, (b) processes the flight, do information to determine air situational equipment and (c) direct weapons to destroy enemy aircraft. The basic architecture of SAGE is similar to modern automated air defense systems A large radar network automatically detected formations of enemy bombers as they approached the continental United States from any direction. Radar sightings are sent over telephone lines to the nearest SAGE command center where they are processed by the AN/FSQ-7 computer.

The communications center would then send warnings and continuous targeting information to air bases best positioned to intercept approaching bombers and surface-to-air missile batteries. The information center also transmits information to neighboring centers and receives them, as well as relays situational awareness to control centers. As the fighters from the air base flew and took off, the control center continuously processed tracking data from multiple probes and sent updated destinations to direct the interceptors to their targets. When the fighters intercepted the approaching bombers,

they sent attack assessment data to the direction center to determine if more aircraft or missiles were needed. While the basic concept of SAGE is simple, the technical challenges are enormous. Currently, one of the biggest challenges is the need to develop digital computers that can receive large amounts of data from various sensors and perform real-time processing to produce target information for interception of aircraft and missiles. To find out if the SAGE project was successful, the researchers created a prototype called the SAGE CAPE COD PROTOTYPE. Shortly after the anti-aircraft program began, Lincoln Laboratory began construction of an experimental system, naming it the Cape Cod system after its location. It is functionally complete; all anti-aircraft functions can be demonstrated, tested and modified.

The Cape Cod system is a model air defense system, which, although smaller in size, actually covers all operational functions. It was time to test the Cape Cod system with live shots. In joint experiments with the MIT Instrumentation Laboratory (now the Charles Stark Draper Laboratory), a B-26 aircraft equipped with an autopilot was connected to a Whirlwind computer and capture vector commands were automatically sent to the autopilot via data link. The robbery went according to plan. The pilot immediately spotted the target aircraft and successfully enabled the autopilot to intercept. Another important first was achieved.1955 was a turning point for the SAGE project, when the focus of the program changed from installing and testing components to testing integrated systems. The style of the program also changed as the Air Force gave SAGE well-defined specifications. The success of the Cape Cod project was still not enough, SAGE's operational plan required a fully functional prototype, and the Cape Cod system was only a simplified model with the most basic tracking and directional listening functions. Supporting Project Sage requires the latest technologies that can detect objects and send them to Central Headquarters for analysis, which is why the Department of Defense (DOD) approved the creation of a Distant Early Warning (DEW) radar, which a. process This project is a successful engineering. and supports the development of SAGE projects by the early 1960s, the SAGE system was fully operational in more than 20 command centers across the United States and Canada. Each center is equipped with a huge AN/FSQ-7 computer.

SAGE enables the US Air Force to monitor and control North American airspace in real-time, providing the capability to detect, track and intercept enemy aircraft. Over time, advances in computer and radar technology resulted in more efficient and smaller systems. The SAGE system, with its thousands of vacuum tubes and enormous size, quickly became obsolete compared to more modern computers. Changes in military strategy and the threats facing the United States also influence SAGE's relevance. The focus shifted from the long-range bomber threat to the intercontinental ballistic missile (ICBM) threat, which required a different early warning system. Missile defense systems such as Nike Zeus and later Safeguard became a higher priority. In the late 1970s, the SAGE system began to be phased out. Battle direction centers began to close, and AN/FSQ-7 computers and other related equipment were scrapped. Although the SAGE system is no longer used, the project had a major impact on the development of computer technology and defense systems. Many of the technologies and concepts developed during the SAGE project became the basis for modern command and control systems (Laboratory, n.d.).

3.3 The Gulf War And The Digital Age

The Gulf War, a significant conflict of the early 1990s, pitted Iraq against an international coalition led by the United States. Beginning on August 2, 1990, Iraq, under Saddam Hussein, invaded Kuwait in a bid to seize control of oil reserves and settle debts from the Iran-Iraq War. The invasion drew swift condemnation from the UN, which imposed economic sanctions on Iraq.

In response to the invasion, the United States spearheaded Operation Desert Shield, a defensive effort lasting five and a half months, aimed at safeguarding Saudi Arabia and other Arab nations from potential Iraqi aggression. President George Bush made it clear that Kuwait's occupation would not be tolerated, deploying American ground, naval, and aerial forces primarily to bases in the Persian Gulf, notably Saudi Arabia. The coalition comprised troops from various nations, including the United Kingdom, France, Canada, Australia, Egypt, Saudi Arabia, and Syria.

With Iraqi President Saddam Hussein failing to meet the UN's January 15, 1991 deadline to vacate Kuwait, Operation Desert Shield transitioned into a military offensive known as Operation Desert Storm. Commencing on January 17, 1991, the operation involved extensive air strikes followed by ground assaults in late February. Advanced military technologies like precision missiles, stealth aircraft, and sophisticated air defense systems were employed, enhancing the coalition's effectiveness while minimizing casualties.

Lasting six weeks, Operation Desert Storm successfully ousted Iraqi forces from Kuwait, concluding on February 28, 1991. Despite its swift and decisive nature, the war left a profound impact, including infrastructural damage in Iraq, a humanitarian crisis, and heightened political tensions in the Persian Gulf region. Moreover, it showcased the widespread utilization of advanced military technologies and intense media coverage, bringing the realities of war directly into homes worldwide and solidifying the United States' dominance in global politics post-Cold War.

One such technology pivotal to the coalition's success was GPS technology, which played a significant role during the conflict. Let's delve deeper into its deployment and impact during the war.

3.3.1 Global Positioning System

GPS is the abbreviation of Global Positioning System. This is a satellite navigation method that can be used to pinpoint a user's location anywhere in the world.

GPS uses signals sent from satellites orbiting the Earth. Signals transmitted from different satellites will simultaneously reach a point on Earth at slightly different times. The GPS receiver calculates its location from a combination of time differences and known satellite directions.

The American military has been experimenting with forms of GPS, for navigation at sea or targeting missiles, since the 1960s. The development of GPS began in the 1960s when the United States Department of Defense (DoD) felt the need to have a navigation system that was accurate, able to function globally, in all weather, and available at all times. Various approaches and technologies were tested until finally at the end of 1973 the US Department of Defense approved the implementation of trials of the Navstar satellite which became the first generation of GPS satellites.

The use of GPS technology in military units was first carried out during the Gulf War by coalition soldiers, GPS was used to navigate in the desert. At that time, the Pentagon ordered 10,000 units and 3,000 units of non-military GPS devices from Trimble Navigation and Magellan Systems, respectively. With a method called "dead reckoning" with reference points being the position of the Sun, stars and planets, then tracking the compass direction and distance traveled, and plotting your position on the map.

To support this new technology in August 1990 during the First Gulf War, American, British, and other coalition troops arriving in Saudi Arabia en route to Kuwait were trained to navigate (Group, 2018).

To measure the distance they have traveled, they learn to count the number of steps they take to cover one kilometer. However, measuring the distance traveled in a tank is more problematic. Although the army had devices to measure speed, it was difficult to drive in a straight line in the soft sand, and this often led to errors.

The use of this technology is very helpful in navigating and determining position. Even food trucks that carry food to soldiers on the front lines use GPS to quickly and easily locate units. The most basic receivers don't include a map, but they do provide accurate latitude and longitude readings, and an indicator to show which direction you're heading. Although this technology has imperfections, it is enough to change the progress of coalition forces.

Until 1983, during the administration of President Ronald Reagan, he permitted the use of GPS for civil aircraft after the shooting down of a Korean Airlines plane, flight 007 which was considered to have "strayed" across the border of the Soviet Union. Since then, GPS has begun to be prepared for use by civilians internationally, especially for aviation and maritime affairs. In subsequent developments, GPS devices continue to be developed to become better, more reliable and more affordable. The way the GPS system works is basically to determine the distance between the positions of the GPS satellites in orbit in outer space to the GPS receiver. With a minimum of 4 satellite signals received by the GPS receiver, the GPS receiver can calculate with an accurate level of accuracy. Currently there are more than 31 satellites with 24 active GPS satellites orbiting in outer space, spread across 6 orbital planes. The signals emitted by GPS satellites contain information on the time when the signal was emitted and also information regarding the position of the satellite in question in outer space. GPS satellites are equipped with jamatoms which have very high accuracy, so that the time data encapsulated in the GPS signal has a high level of precision/accuracy (Sutrisno, 2021).

3.4 Contemporary Cyber War

From World War II through the Vietnam War, warfare entered what Antoine Bousquet terms the "Cybernetic Warfare" period. This era was characterized by total war efforts, involving the full mobilization of national resources and the deployment of complex communication networks and logistical support systems. Cybernetic warfare relied on computerized systems integrated with electronic communication channels to coordinate military activities (Anwar, 2015).

However, following the United States' defeat in Vietnam, new approaches emerged, particularly in facing asymmetric warfare challenges. "Chaoplexic Warfare" arose, designed to counter small, highly mobile enemy forces with flexible command structures. While still leveraging electronic communication and computer systems, this form of warfare emphasized adaptability, change, and positive feedback. Key considerations included nonlinearity, self-organization, and emergence, embodying an adaptive system approach and utilizing network-centric warfare strategies.

Future wars, influenced by the Revolution in Military Affairs (RMA) theory, are expected to rely heavily on long-range guided missiles, potentially incorporating bacteriological warfare. Concepts like "space control" and an "empty battlefield" are discussed, with a growing emphasis on unmanned aircraft in US force planning.

Military historian Jeremy Black predicts continued potential for future conflicts, driven by the significant increase in global population levels. With estimates projecting a rise to 8.9 billion by 2050, competition and rivalry among nations for resources to meet their populations' needs are expected to intensify. While cooperation in resource exploration may occur, this rivalry could lead to serious confrontations as countries seek to defend or seize resources, potentially escalating conflicts on a large scale.

The relationship between war and technology is reciprocal, with warfare driving technological advancements in weaponry and vice versa. The emergence of cyber warfare exemplifies this dynamic, utilizing computer networks and the internet to conduct defensive and offensive operations in cyberspace. Cyber warfare involves actions such as disrupting communication, altering information flow, and influencing public opinion through online campaigns, propaganda, and agitation, all without the resource-intensive requirements of traditional methods (Soewardi).

3.4.1 Cyber warriors

With the formation of National Cyber Defense, it is hoped that national capacity building in order to increase national resilience against various threats from the cyber world will be further improved. Infrastructure development also needs to be immediately realized in an integrated manner, preparation of concepts and initial development or a comprehensive Cyber Defense Backbone, considering that so far The development of the Cyber Defense concept is still sectoral or not yet comprehensive as a single National Cyber Defense unit.

the fact that after several years of modern war today, as has been carried out by American troops and their coalition (NATO) in various military operations in various countries (Iraq, Afghanistan, Somalia, Serbia, Bosnia and others), apparently has not guaranteed success in controlling the situation or overall (absolute) control of the situation. So a question arises, can only modern military technology implemented in the concept of cyber warfare be able to win a war?

Cyber attacks targeting one country have also occurred in Estonia and Ukraine, these attacks were able to paralyze vital infrastructure in both countries. Researchers and technicians conducted research and finally found the internet which could be used as a forum for communication and accessing the necessary data. The trend of war is shifting by optimizing the use of science and technology (IPTEK) so that previous wars or conventional wars between countries are almost no longer found, but the war that is more dominant is cyber war.

3.4.2 CASE STUDY

An example of the case is Russia vs Estonia. In 2007, it started on April 30 2007, when the Estonian government removed a statue of Stalin. The statue's movement sparked tensions between Estonian civilians and the Russian minority. For Estonian civilians, the statue represents Russia's oppression of Estonia, while for the Russian minority, the statue's movement to the outskirts of Tallinn represents their ethnic marginalization. The removal of the monument led to increased resistance against the Estonian government. The attackers had about six months to plan their attack in protest of the event. The attackers prepare for cyber attacks and riots, and ensure them through a planning process.

Nashi Youth Group carried out a cyber attack using Distributed-Denial of Service (DDoS). by targeting several important sites such as the presidential website, the Estonian parliament, the Estonian Police, Political Parties, and very influential mass media. The timing and apparent coordination of the cyber attacks and riots suggest they were highly organized. During the cyberattack in Estonia, Russian-language forums provided news updates and a recruiting ground for interested hackers. This shows that digital technology enables rapid transnational mobilization in times of crisis. On the other hand, there are Russian language forums with downloaded tools and instructions on how to carry out cyberattacks.

Based on the Cyber Early Warning model which was linked to the Russia vs Estonia war, latent tensions between the two countries were in the form of the removal of the Stalin statue and its barrage, then cyber recon by gathering information through online forums and initiating events, shown by preparations carried out for approximately six months. In this case, the author assesses that the attacker first looked for information about the target/opponent (Estonia) either through online groups/special forums or other means, then planned a DDoS attack. To maximize the attack and maximize the impact of the attack, the attacker carries out cyber mobilization by providing a recruiting ground for interested hackers as well as special tools and instructions for carrying out cyber attacks.

The latest case: Tensions in 2022 between Russia and Ukraine became increasingly volatile after Russia invaded Ukraine in February 2022. In the perspective of the Cyber Early Warning model which is juxtaposed with the Russia vs Ukraine cyber war, it can be seen that Russia is still using the same pattern when carrying out cyber attacks against Estonia in several years ago.

The dispute between the two countries is basically not a new conflict because disputes between the two countries ranged from small to large several times after the Soviet Union collapsed and the two countries became independent countries. A number of border problems such as Russian cyber attacks on Ukraine, separatist movements, and Russia's annexation of territory. Apart from that, the conflict currently developing in Ukraine is a geopolitical symptom triggered mainly by the West under the control of the North Atlantic Treaty Organization/NATO.

Russia launched an extensive cyber campaign shortly before the invasion, with reports indicating a major increase in exploits on the first day with the aim of creating chaos and disrupting Ukraine's defenses. Russia attempted to disrupt services and installed destructive malware on Ukrainian networks including phishing, and exploiting software vulnerabilities. Microsoft's Ukraine Special Report notes that since the invasion, several hacking groups connected to Russia carried out hundreds of cyberattacks against Ukraine. The hacker group began hacking preparations in March 2021.

At the latent tensions stage, the problems that emerged were border issues and geopolitical symptoms resulting from NATO intervention. Next, the cyber recon stage is carried out by collecting information through cyber attacks which reach hundreds of attacks. Then at the initiating event stage, preparations were carried out for quite a long time, almost a year before the Russian invasion of Ukraine. The next stage is the cyber mobilization stage by obtaining support from a hacker group from Russia with the target of cyber attacks on Ukraine (Samad & Persadha, 2022).

3.4.3 STUXNET

Stuxnet is a worm that specifically attacks Windows-based computers. On 20 and 23 November 2010 the Iranian military officially declared that the worm Stuxnet attacks Natanz (Iranian nuclear facility). This worm even managed to remote a dangerous

explosion at the uranium enrichment center of the nuclear developing country. This incident was allegedly carried out by Israel and the United States as the main opponents of Iran's nuclear program. cyber war between Indonesia and Malaysia. Mutual infiltration between hackers from both countries. Although the governments of the two countries did not involve the hackers' actions, they attacked cyber facilities belonging to the Malaysian and Indonesian governments.

Based on the 2021 Cyber Security Monitoring Annual Report, the National Cyber and Crypto Agency (BSSN) recorded 1,637,973,022 anomalous traffic with the highest traffic in December being 242,066,168 anomalies, 264 phishing cases, 5,940 web defacement cases with the most cases occurring in March which reached 727 cases, and as many as 1,676,286 Advanced Persistent Threat (APT) activities in Indonesia (Directorate of Cyber Security Operations 2021)..

However, Indonesia is continuously building the strength of its armed forces with the aim of defending its country and nation from all threats and disturbances, both those coming from abroad and those emerging from within the country. This strength is built by utilizing available national resources until it reaches a level of strength that has an adequate deterrent effect. For Indonesia, war is the last resort if diplomatic efforts to defend vital national interests fail.

3.5 Impact and Implications of Computer Technology in War

3.5.1 Technological Excellence

Technological superiority in the military field is very influential for the superior party. The use of technology in the military field can have a very significant impact. The first use of communication systems, before the development of radio systems, was to convey messages manually. On the battlefield, conveying information manually is very risky because soldiers have to deliver the message in the middle of a dangerous battlefield. If the soldier assigned to deliver the message falls, it can be guaranteed that the message will never reach its destination. After radio technology was developed, the communication system became better because radio waves could send messages in the form of sound instantly. However, the use of radio also faces obstacles because radio wave signals can be picked up by the enemy which can provide the enemy with beneficial information. Currently, sending information uses an internet network that is more modern and safer than using radio. The use of technology also helps in intelligence gathering.

Not only for collecting valuable intelligence, technology can also help break secret codes that can provide valuable information and increase a country's intelligence defense. With an internet network architecture created in such a way, the process of recruiting, monitoring and gathering information from intelligence is expected to be safe and easier. Internet technology is a win-win solution for training and educating soldiers. This is because with this technology, soldiers can not only be educated using webinars, but can also be trained using various simulations, whether flight simulations or even battle simulations. With simulations like this, soldiers will not only be trained, but also trained without risks that threaten their physical and mental health.

Technology also helps manage the logistics required during military operations, the use of calculators and electronic computers speeds up the calculation of resources needed by military personnel. Technology is also used to optimize weapons such as controlling long-range bullets (Ballistics, Cruise, etc.). Technology makes it easier for personnel to navigate the battlefield

3.5.2 Ethics and Security

From an ethical perspective, the use of autonomous weapons systems and computer-controlled drones raises serious questions regarding responsibility and lethal decisions made by machines. For example, who should be held responsible if an autonomous drone makes the wrong decision and causes the death of a civilian? This issue is increasingly complex with the development of artificial intelligence (AI), where systems can make decisions without direct human intervention.

Additionally, advanced surveillance technologies, such as facial recognition and tracking, can be used for military purposes, but can also be misused for mass surveillance of civilian populations. This raises concerns regarding privacy and human rights. On the one hand, this technology can help prevent threats and maintain national security; on the other hand, uncontrolled use may violate individual privacy and civil liberties.

The issue of disinformation and propaganda also arises along with the use of computer technology in war. Countries can use social media and other digital platforms to spread false information, influence public opinion, or cause chaos within enemy populations. This technique, often referred to as “information warfare,” can undermine democratic order and exacerbate conflict.

The Future of Technological Warfare

2024 is part of the industrial revolution 4.0. A digital industrial era where all parts in it collaborate and communicate in real time anywhere at any time with the use of IT (information technology) to produce new innovations or other optimizations that are more effective and efficient

According to Schlechtendahl, Industrial Revolution 4.0 emphasizes the element of speed in providing information. All entities in the industrial environment are always connected and ultimately share information with each other. So according to Schlechtendahl, the Industrial Revolution 4.0 opens up opportunities for all entities in industry to communicate with each other in real time.

2018 is the initial milestone of the industrial revolution 4.0. The industry combines automation technology and cyber technology. So, in this situation it is possible to exchange data in manufacturing technology. In this era, virtual worlds are possible that form the connectivity of humans, machines and data. Industrial Revolution 4.0 can be interpreted as a phenomenon that combines cyber technology and automation technology.

also called a cyber physical system.

Some of the advances that emerged in the Industrial Revolution 4.0 era are artificial intelligence, nanotechnology, biotechnology, blockchain, internet-based technology, quantum computer technology, and 3D printers.

The five main pillars in the Industrial Revolution 4.0, namely the Internet of Things, are defined as a system that utilizes computing devices, mechanical devices and digital machines that are simultaneously connected to each other (interrelated connection). Big Data is the term used to describe large volumes of data, both structured and unstructured. Artificial Intelligence is machine computer technology that has artificial intelligence like humans. Cloud Computing and Additive Manufacturing are new breakthroughs in the manufacturing industry using 3D printer machines or also known as 3D printing.

Of the five main pillars of the industrial revolution 4.0, there is a main pillar or first pillar that allows the development of the other four pillars, the first pillar is called the Internet of Things (IoT). Internet of Things (IoT) is a concept where an object has the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. According to Casagras (Coordinator and support action for global RFID - related activities and standardization) defines IoT as a global network infrastructure, which connects physical and virtual objects through the exploitation of data capture and communication capabilities.

With the rapid growth of technology and its influence on every aspect of human life, the defense and military aspects are also not spared. The development of technology is also utilized by the military to strengthen strategic and crucial areas for operational excellence and effectiveness.

Artificial intelligence (AI) will play a key role in changing the face of war. AI algorithms will enable faster and more accurate data analysis, helping the military to better identify enemy movement patterns and predictions. AI will be used in autonomous weapons systems, drones, and combat robots, enabling operations without direct human intervention. This not only increases efficiency but also reduces risks for military personnel. However, there are concerns regarding the ethics and responsibility of using autonomous weapons that can make lethal decisions.

The use of robots and autonomous systems will become increasingly common in military conflicts. Autonomous combat robots and drones will perform a variety of tasks, from reconnaissance to direct strikes, with advanced sensors and navigation capabilities that increase effectiveness on the battlefield. This automation not only increases operational capabilities but also reduces risks to human forces.

Computer technology will be used to spread information and disinformation through social media and other digital platforms. States can influence public opinion, cause chaos, or undermine political stability in enemy countries. This information war will affect the democratic order and exacerbate conflicts.

Overall, computer technology will continue to change the face of warfare, making it more sophisticated, faster, more integrated and more lethal. However, success in adopting this technology will depend on the ability of militaries and states to manage the risks and associated ethical issues (Linknet, n.d.).

4. CONCLUSION

The use of technology in the military field has been proven to be able to strengthen military forces, such as the use of the Colossus and ENIAC machines which helped the Allies break secret German codes in World War II, improving air defense systems such as the SAGE project created by America on the basis of a computer system to improve defense. the air anticipated if the Soviet Union's planes would attack, the use of GPS in the Gulf War which was proven to help soldiers navigate in the desert, to the use of the internet as a weapon and propaganda in the digital era. The use of technology has been able to improve every aspect of human life. The use of technology in war has changed the course of war from war with large mobilization of citizens and resources (total war), but all that has changed since America's defeat in the Vietnam War which changed the way of fighting to mobilize as little as possible by utilizing technology to get results. as much as possible. This event was the beginning of cyber war, namely a type of war that uses the internet as a weapon and national defense. This type of war has proven to be more economical than total war. This war relies on technology such as computers, spy satellites, automatic weapons and also artificial intelligence. However, there is still debate among experts that a small error in a computer system or artificial intelligence can have an impact on many human lives. From the beginning of World War II, which claimed many victims, it cannot be denied that with the war, technological progress developed very rapidly, perhaps if there was no war, the technology we have now would not be as advanced as it is now. However, war cannot be justified because the victims are humans themselves.

REFERENCE

[1] Anwar, S. (2015). PENGUASAAN TEKNOLOGI PERTAHANAN OLEH SDM PERTAHANAN INDONESIA DALAM RANGKA MENGHADAPI PEPERANGAN MASA DEPAN. *jurnal pertahanan dan bela negara* , 15-34.

[2] Copeland, B. (2024, january 25). *Colossus*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/technology/Colossus-computer. Accessed 22 May 2024.

[3] Group, S. M. (2018 , november 2). *GPS Navigation: From Gulf War to Civvy Street*. Retrieved from Science Museum: https://www.sciencemuseum.org.uk/objects-and-stories/gps-navigation-gulf-war-civvy-street

[4] hapsari , r., & adil, M. (2018). *Sejarah SMA/MA kelas XII kelompok perminatan ilmu pengetahuan sosial*. Retrieved from brainly : https://brainly.co.id/jawaban-buku/q-

jelaskan-perlombaan-teknologi-terjadi-amerika-serikat-uni?source=qa-qp-match

[5] kids , b. (2024). *Persian Gulf War*. Retrieved from britannica kids: https://kids.britannica.com/scholars/article/Persian-Gulf-War/59340

[6] Laboratory, M. L. (n.d.). *SAGE: SEMI-AUTOMATIC GROUND ENVIRONMENT AIR DEFENSE SYSTEM*. Retrieved from mit lincoln laboratory: https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system#

[7] leese, b. (2023 , september 28). *THE COLD WAR COMPUTER ARMS RACE*. Retrieved from marine corps university press: https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-14-no-2/Cold-War-Computer-Arms-Race/

[8] Linknet. (n.d.). *Manfaat Internet di Bidang Militer* . Retrieved from liknet : https://www.linknet.id/article/manfaat-internet-di-bidang-militer

[9] Samad, M. Y., & Persadha, P. D. (2022). Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara. *Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi)*, 135-146.

[10] Soewardi, B. A. (n.d.). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *media informasi ditjen pothan kemhan*, 31-35.

[11] Sudirman , I., & Wahono , R. S. (2003). *Sejarah Komputer*. IlmuKomputer.Com.

[12] Sutrisno, L. (2021). ANALISIS DAN PERANCANGAN APLIKASI GPS BERBASIS ANDROIDUNTUK CV. EXPRESS TRI'YO MUJUR. *Jurnal Informatika dan Bisnis*, 69-80.

[13] Swaine, Michael, R., & Paul, A. (2024, may 3). *ENIAC*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/technology/ENIAC. Accessed 22 May 2024.

[14] swift , j. (2009, maret). *The Soviet-American Arms Race*. Retrieved from history today : https://www.historytoday.com/archive/soviet-american-arms-race

[15] wikipedia. (2024, april 22). *ENIAC* . Retrieved from Wikipedia : https://p2k.stekom.ac.id/ensiklopedia/ENIAC