The Seybold Report

ISSN 1533-9211

CYBER WARS AND GLOBAL SECURITY CHALLENGES

Dr. HAZIM JERRI MNEKHIR

Ministry of Higher Education and Scientific Research (Department of Scholarships and Cultural Relations). Email: hazim.jerri@scrdiraq.gov.iq

Abstract

War, perhaps this word is one of the oldest known to humans, not only witnessed all stages of the rise and decline of states and empires, but also due to the large number of its victims and the diversity of its methods and tactics. Or indirect, and in all its cases, war is a phenomenon mixed with violence, hostility and destruction, and it may be held for mostly political or even military goals. Wars are either comprehensive and long or limited and rapid, and in the light of technological development, the methods and tools of war have gradually evolved until they reach cyber warfare that We will present what information we can in this chapter, and we hope that it will gain your approval. The first topic will focus on the development of war and its generations until it reached the fifth generation, then its patterns, types and weapons, and then the second topic between the forms of threats and cybercrime against international actors, institutions and individuals, and then The third topic: between cyber deterrence and countries and its tools, and countries that have cyber armies or cyber security councils, and conclude the chapter With The Impact Of Cyber Attacks On Global Security.

Keywords: Cyber Wars, Global Security Challenges.

THE FIRST TOPIC: THE DEVELOPMENT OF WAR AND CYBER WARFARE

First: definition and concept of cyber warfare

Defining cyber war: There is no broad consensus on a specific and precise definition of the concept of cyber (electronic) war.

The US Department of Defense defines cyber war as “the use of computers and the Internet to conduct war in cyberspace.” It was one of the most famous writings that predicted cyber war. For each of them, "John Arquilla and David Ronfeldt", in their article published in 1993 entitled, "Cyber war is coming" when he warned that cyber war is coming, and the two authors knew:

- **Cyberwar:** Executing or preparing to carry out military operations, according to informatics principles, by disrupting or destroying information and communication systems on a large scale. Rather, the authors expanded the concept of cyberwarfare to include also non-material dimensions represented in the destruction of the enemy's military doctrine, which represents The basis on which his identity, plans, actions, goals and challenges he faces depend on, through the other side, and shifting the balance of knowledge; To be in the interest of this party, cyber warfare is the process of employing knowledge with the aim of harming the opponent (1).
- **Joseph Nye defines cyber warfare as:** "Hostile acts in cyberspace that have effects equal to or greater than conventional kinetic violence" (2).

The Seybold Report
ISSN 1533-9211

- **The concept of cyber warfare**: conventional wars have changed, and military armies around the world are concerned with information security and their role in future wars, which are expected to take place in cyberspace, and maneuvers are being conducted to train on this new type of conflict and how it can be confronted and prepared. It has, in order to penetrate the national sovereignty of any country, obtain intelligence information, recruit agents, etc., and that the nature of war does not change, but the characteristics of war can change with the development of war tools, the emergence of drones, and what is called war without fire, smoke, or bombing However, it has a violent side in terms of penetration, piracy, spreading viruses and other methods, and despite the huge losses it causes, cyber weapons are simple and often do not exceed "kilobytes", which is what electronic viruses represent that penetrate the computer network and spread quickly.

Second: Generations of War: Cyberspace The Fifth Field of War:

The four domains that were known in the traditional armed confrontation between the countries of "land, sea, air and space" are no longer alone in the international arena. Rather, a fifth domain of this confrontation has entered, which is "cyberspace". It is expected that "Cyber War" will be the dominant feature, if not the main one. For future wars in the twenty-first century, and the danger of Internet and network wars lies in the fact that the world has become more and more dependent on cyberspace, especially in the military, banking and government information infrastructures, in addition to public and private institutions and companies.

There is no doubt that the increase in electronic attacks, of which we are witnessing a small part today, is also related to the increase in this dependence on computer networks and the Internet in the basic national infrastructure, which means that electronic attacks can develop today to become a decisive weapon in conflicts between states in the future, bearing in mind that the dimensions of the concept of war Electronic is still not understood by a wide range of observers and the public (5). A number of experts, within their specialties, have endeavored to provide a definition surrounding this concept. Richard Clarke and Robert Knacke defined electronic warfare as “actions carried out by a country through which it attempts to penetrate computers and networks belonging to another country with the aim of achieving severe damage or disabling it.”). It is expected that cyber warfare will become a model sought by many countries due to the many characteristics it entails, including:

Cyber wars are asymmetric wars: The relatively low cost of the tools needed to wage such wars means that there is no need for a country, for example, to manufacture very expensive weapons such as aircraft carriers and advanced fighters to pose a serious and real threat to a country like the United States of America. For example, it needs capabilities that may cost as much as a tank (6).

1- The first generation of war 1G. W classic conventional wars:

They are the familiar wars since the dawn of history, and they are direct confrontations between two armies that adopt methods of attack, defense, siege, circumvention, ambush, raid, duel, naval confrontation, artillery bombardment, and direct warfare (8).

The Seybold Report
ISSN 1533-9211

2- The second generation of war 2G. W Total Wars:

That America has manufactured two atomic bombs, one of which relies on atomic fission, and the other relies on atomic fusion, and the American President "Harry Truman" claims the third president of the United States of America, with his call to strike Japan, because it is already losing, and it flees from the regions it occupied in Asia and its defeat became a matter of time Only, and the bomb had been completed during the reign of President "Franklin Roosevelt," the president who preceded him, and who died at the beginning of his fourth term before deciding the outcome of the war, but the generals insisted strongly, considering that there was no value in possessing a mighty weapon, without the world realizing its power and seeing its destructive effects. All military and civilian

targets are legitimate targets, and the whole world will be directly affected in these wars by the battles, which are the wars of aerial bombardment, trenches, lightning wars, the deadly comprehensive blockade, the deadly economic sanctions, the propaganda war, the psychological war, spies, the burning land, genocide, and the international alliances that include dozens of countries, and they are wars that are not It ends only with annihilation or surrender, and it is direct confrontation wars that are characterized by the supremacy of the high patriotic spirit and that they are between regular armies (9).

3- Third Generation Wars (3G.W.) Cold War:

Some define it as preventive or preemptive wars, such as the war on Iraq, for example, and the American expert William Lind defines it as being developed by the Germans in World War II. It also came after World War II. It was marked by the Cold War between the Eastern Bloc, led by Russia, and the Western Bloc, led by America. The theater of this war is the entire world and its character is proxy wars such as the war in Korea, Vietnam and Afghanistan, comprehensive ideological propaganda wars, economic wars, military coups, and spinning in the orbit of one of the two blocs. It is also distinguished by a new phenomenon, which is the wars of popular liberation from colonialism or from tyrannical regimes (10).

4- 4G. W wars:

The first factor: the political employment of terrorism: The period between the late twentieth century and the early twenty-first century marked the beginning and spread of the phenomenon of terrorism at the international level. International policy to confront this phenomenon. Terrorism in 2001 was a danger that must be eliminated, but today it has become a necessity to justify the continuation of new military institutions. Fear of terrorism was the natural feeling of the population because they are affected by its crimes. It does not exist, everything has become permissible to justify the continuation of the military institutions that bear the name (joint unity). We are facing a real field war that no one mentions in the American or international press except in an occasional and unfocused manner. It is a war in all its meanings and it may be brought to the fore at any moment, especially If a journalist who wants quick fame, or a senior political authority who is damaged, or a certain intellectual or political center of influence succeeds, how can armies be recruited and wars waged in many countries without raising even the slightest level of questioning?

The Seybold Report
ISSN 1533-9211

The strange thing is that terrorism did not exist in Iraq, Somalia, Yemen, Libya, or Syria, so how did the circle of terrorism expand in this systematic manner, so that groups of terrorists from more than eighty-five countries appear on the Syrian scene, fighting the existing regime there, practicing ethnic cleansing, and demanding Democracy! Then a phenomenon similar to its neighbor Syria appears on the Iraqi scene! Then an Islamic state appears that brings a "caliph" to the Muslims, and succeeds within weeks in controlling nearly a third of the area of Iraq, and half of the area of Syria! The number of elements included in the list of terrorist operations in the Islamic region in general is too great for anyone to be able to classify them as a matter of coincidence, especially when we remember that supply, armament and financing are too great to escape the eyes of American control and intelligence. The continued growth of the circle of terrorism in the geography of the world is certainly not a coincidence that fear of terrorism in these circumstances is legitimate. However, it is permissible to ask at the same time about the party that should be afraid, and it is clear that the peoples of the region in which terrorism wreaks havoc are the ones who are at risk in the first place, that this international terrorism, and the rate of its spread, arming and financing, cannot have been repeated and spread purely. coincidence. It must have threads, pulled and moved by steady and strong fingers, and purposeful conscious brains. The fourth generation was known to target civilians, not as usual in previous generations. (11).

The second factor: is the use of psychological operations: psychological operations in the fourth generation are similar to leaflets in the old wars, in which the soldier used to throw his leaflets from the plane at the army to call them to despair and surrender, in modern wars he does not use this method and targets the civilian sector and the military also with bad or very negative propaganda There are three persuasive steps: it shows that there is a bad situation, that today is bad, that there will be a much worse tomorrow, and that your tour will not provide you with a better life, and therefore change must be made, (12).

The third factor: Public opinion: Influencing and controlling public opinion is a new weapon that major powers have mastered in using, especially in third world countries. It brought down countries, influenced others, and terrorized thirds.

In order for the process of change to work, and then he will certainly hijack this change in his favor, but the mobilization process in the street is always characterized, and as soon as people take to the street, people of the demonstrators must be killed in mysterious circumstances, and always the first accused are the security services loyal to the existing regime, and therefore there is an additional reason for the demonstrators To escalate, and it may become a collision and international intervention, as happened with Libya, Syria and Yemen.

The fourth factor: is the use of civil society organizations:

And they are used for the benefit of the enemy, not all of them, but some of them help in reading the society from the inside, so that they can understand the society and its behavior.

The fifth factor: the hidden foot strategy: which is putting the target country under constant pressure with the rumor and focusing on the mistakes of its various agencies, whether security or non-security. Here, the fourth generation wars have another advantage, which is not knowing

The Seybold Report
ISSN 1533-9211

who is doing this directly, as it is called the "hidden foot strategy", meaning that they are wars Indirectly, you know your enemy, but you cannot prove it easily. When we understand the dimensions of the fourth generation, we always see a blurry area of who is right and who is wrong. One of the mechanisms of the fourth generation is to make each party question the intentions of the opposite party. There is always a blurring of who is right and who is wrong (13).

5- Cyberspace is the fifth domain of 5G. W war:

At the beginning of the twentieth century, the world witnessed a frantic arms race between many traditional and emerging international powers at the time in Europe and South America, which led, among other reasons, to the outbreak of the First World War and the use of new mechanisms and tactics in the fields of war and the resulting change in the political map (It is very similar to what the world is currently witnessing from an arms race of another kind in a new field, which is the field of cyber warfare, which is tainted by ambiguity and uncertainty. The role of the air force in wars, and it was said that cyber warfare is taking place now, and its battles are conducted in secret at times, and with deafening noise most of the time, although no one calls it by its name directly. Sometimes, statements are issued by the leaders of “NATO” and the US military and their counterparts in Russia and China, about non-stop cyber battles via the Internet, and they are run by command centers that have become independent of their armies, especially in the United States, Russia and China. However, it must be noted that cyber wars, which have not ceased to be talked about, are only part of the "fifth generation wars". The features of these wars were not completed until after the discussions about the Russian electronic interference in the US presidential elections in 2016 that brought President Donald Trump to the presidency, which quickly intensified the discussion publicly in the “Hybrid Wars” leading up to the “Helsinki Summit” in July (July) 2018, which represented an unexpected station in the fifth generation wars (14). Perhaps a clear example of this emerged in the “ISIS” organization’s control over large areas of Syria and Iraq and its rule beginning in 2014 (under the name of the “Caliphate State”). The “Boko Haram” movement in Nigeria followed a similar approach in that same year (15).

International reports said that the executive order issued by US President Donald Trump to the Ministry of Defense to launch successive cyberattacks on Iran's systems and computers is tantamount to causing a complete paralysis of the defense systems that Iran uses to resist possible military strikes, with evidence that Trump stated that he did not back down from the military strike. But he has stopped it for the time being (16).

The Washington Post quoted sources as saying that Trump ordered the Pentagon this week to launch electronic strikes that took down Iranian computer networks used to control missile launches, after Iran shot down an American surveillance drone that it said was violating its airspace. The sources said that the electronic strikes, which took place on Thursday night against the Revolutionary Guards, could greatly threaten the Internet networks in Iran, and at the same time preserve American tankers and oil supplies in the Gulf region, in the meantime, a report by "cnet" said that the American army can To sink hostile Revolutionary Guard ships every 24 hours if necessary through electronic attacks, and the report indicated that the "US

The Seybold Report
ISSN 1533-9211

Cyber Command" moved from a defensive position to an offensive position, according to the Military Authorization Act passed by Congress in 2018, which gives the green light to deter any A "secret military activity" in cyberspace is to protect and defend US interests. Cyberattacks are a means of pressuring the enemy and paralyzing it completely, in preparation for a military strike or a land or sea invasion. It is highly effective, given that it paralyzes the enemy's systems, in which modern technologies are used. And Iran has recently chosen international isolation, as many airlines around the world have modified their air routes, because of what insiders said, in order to avoid the electromagnetic field surrounding it, because of which the navigation systems of airlines may be affected and be disturbed, so cyber warfare, according to analysts, depends on generation war makers. Fifth On the use of modern technologies, ranging from armed force, such as anti-tank missiles, suicide operations, ambushes, and terrorist acts, in addition to electronic technologies, which are a key player, and are being moved according to the political goals of other countries, and experts believe that one of the reasons for the emergence of wars The fifth generation is the development of the media, as it is exploited in managing relations between states, and creating public opinion opposed to the political authority in the state, in order to weaken its ability to control and control the relationship between society and the state, and the cost of such wars is less expensive than the use of force Military, because it drains the economic power of states (17).

The second requirement: geocyber

First: the geopolitics of cyber warfare

Written by Christina Kosch, Senior Resident Scholar at the German Marshall Fund (□) Most of the transatlantic discussion of national security, from a geopolitical angle, has focused on Russia and its interference in Western elections. abroad using electronic tools. With the entry of digital into various industries, geopolitics has become the use of political skill to gain influence in international affairs far from its original geographical framework. Cyberspace, the global network of interconnected information technology including hardware, software and information, hosts some of the most important weapons and geopolitical vulnerabilities of nations alike. Since it is not possible to differentiate between electronic and physical threats, cyber geopolitics is likely to be at the forefront of geopolitics in the future, but cyber-attacks are very different from traditional tools with international influence in the geopolitical battlefield in many other respects. These attacks have a high capacity for sabotage at a relatively low economic cost to the attackers. Likewise, the political cost in the form of the possibility of exposure to the risk of retaliation is very low, given the challenges facing the possibility of identifying those who carried out the attack. Also, the international law’s omission of categorical sanctions and texts to confront cross-border cyber operations makes it more attractive to some, as it combines high destructive capacity and rapid spread at a low political and economic cost. specific defensive (23).

The Seybold Report
ISSN 1533-9211

Second: Interrelated and Interpretive Frameworks First: Cybersecurity:

The increase in the interdependence between security and technology has made the strategic international interests of states in danger and a constant threat, which has made cyberspace a mediator and a source of tools for international conflict. and the absence of fear of the danger of these values being attacked (). That the availability of cyberspace security is achieved in the event of the existence of protection measures against exposure to hostilities, and the misuse of communication and information technology (26). Accordingly, cyber security put in place the measures and strategies taken to prevent information from reaching the hands of unauthorized persons through communications, and to ensure the authenticity and authenticity of communications, a strategy must be developed to protect them, because the nature of that space as a global arena that crosses the borders of states, made cyber security extend from within states to The international system to form a kind of global collective security, especially with the presence of risks threatening all actors in the global information society, so there has become an international interest in protecting the security of cyberspace, given that this space has become part of global security, and this view is supported by the changing nature of electronic interactions, Especially with the development of human artificial intelligence and the ability to produce new technologies, as well as the escalation of the dangers of electronic threats to the global infrastructure of information (27).

The interest in cybersecurity was not limited to the technical dimension only, but also extended to other dimensions of a cultural, social, economic, military, and other nature, especially since the non-peaceful use of cyberspace affects the economic prosperity and social stability of all countries whose infrastructure has become dependent on Cyberspace, and the decline of state sovereignty with the escalation of the role of non-state actors in international relations (such as transnational technology companies, crime networks, electronic piracy, terrorist groups, etc.) posed numerous challenges in maintaining global cybersecurity, and prompted the emergence of Pluralistic directions to achieve that security through coordination between stakeholders from governments, civil society, technology companies, the media, and others (28).

Third Frame: Cyber Conflict:

The phenomenon of "conflict (□)" has undergone changes with the emergence of cyberspace, as a field in which conflicts arise between different actors, after the

heavy reliance on communication and information technology. Non-states in cyberspace, and despite the effects that may be devastating to this type of conflict, it is not accompanied by blood, and it mostly includes espionage and infiltration of opponents' electronic sites, and hacking them without rubble or dust, and its parties are characterized by lack of clarity, and it affects in many dangers to the security of the state, through cyber attacks (29).

The spread of cyberspace, and the ease of automatic entry, led to the expansion of the circle of cyber conflicts, and then led to an increase in the number of attackers, and there is a state of hit-and-run in cyber attacks to express the protracted conflict (30).

The Seybold Report
ISSN 1533-9211

1- **Cyber conflict of a political nature:** This conflict is clearly motivated by political motives, and sometimes it evolves to take a military or defensive form through cyberspace, by corrupting the opponent's information systems and infrastructure networks, and this type of conflict is usually employed. , cyber weapons by actors within cyberspace, or by collaborating or employing other forces to achieve political goals (33).

2- **A cyber conflict of a soft nature:** This conflict is how to obtain information from the opponent, and how to use it and employ it in waging a psychological and media war. Sometimes this type causes an international crisis, as happened when WikiLeaks published documents that caused an international diplomatic crisis.

Cyber conflict over technological progress: This conflict takes on a competitive nature over supremacy in artificial intelligence or technological development, theft of scientific secrets, and competition over patents.

The third requirement: types of cyber warfare

First - Multiple types of cyber warfare:

1- The first type: "low-intensity" cold cyber war:

Cyberspace is an arena for low-intensity conflict, and this conflict is continuous between the actors, and it may be of an extended nature, and permanent hostile or non-peaceful activity, and it is described as having deep and intertwined roots, and it has multiple economic, social, and cultural aspects, and soft power is often resorted to. For cyber wars in such conflicts, although they do not evolve into conventional wars in most cases, or waging a comprehensive cyber-war, the cold cyber-war is always characterized by many means, such as psychological warfare, espionage, penetration, theft of important information, waging wars of ideas, and competition between international companies and international intelligence services. This pattern was manifested in war situations in political conflicts with a social and religious dimension. The extended conflict, such as the Arab-Israeli conflict, the Indian-Pakistani conflict, or the conflict between North and South Korea, and other ongoing conflicts, and in light of these conflicts, international piracy groups are active to express political or human rights positions, such as the "WikiLeaks" and "Anonymous" group, as well as Also in cases of international crises, such as the tension between Estonia and Russia in 2007, as well as the mutual penetrations between China, the United States and Russia, or between Tehran and Washington (36).

2- The second mode: the "medium-intensity cyber warfare" mode:

As the conflict in cyberspace turns into an arena parallel to a conventional war on the ground, and this is an expression of the intensity of the conflict between the parties, and this may pave the way for military action, and the cyberspace war takes place by hacking cyber sites, sabotaging them and waging psychological warfare against opponents, These cyber wars derive their intensity from the strength of their parties, and their association with conventional military actions, and some estimates indicate that the cost of cyber wars is cheap, and an entire cyber campaign may be funded at the cost of a tank. As for the use of this type of medium-intensity cyber warfare, it was used in 1999 by NATO NATO invaded Yugoslavia, and cyber attacks

The Seybold Report
ISSN 1533-9211

aimed at disrupting communications for opponents as well, emerged during the war between Hezbollah and Israel in the year (2006), as happened between Russia and Georgia in 2008, and the confrontations between Hamas and Israel in the years 2008 and 2012 (38).

3- The third pattern: "hot cyber war of high intensity":

This type of war, when it arises in cyberspace, is considered isolated, and it is parallel to conventional military actions, and so far the world has not witnessed.

Second: Cyber risks and repercussions:

The expansion of the relationship of countries with cyberspace, and the resulting cyber wars, led to many risks to national security and the transition to international political interactions, the most prominent of which can be put forward

1) The spread of cyber risks, especially in the vital installations of countries, whether they are civil or military, and this is done through an intermediary and
2) carrier of services, as he shapes their information systems, which affects the functions of those facilities and therefore whoever has control over the cyber force to carry out attacks, he Has strategic control of great importance, whether in times of peace or war (40). (45).

And Afghanistan, comprehensive ideological propaganda wars, economic wars, military coups, and rotation in the orbit of one of the two blocs, as distinguished by a new phenomenon, which is the wars of popular liberation from colonialism or from tyrannical regimes (46).

And that your tour will not provide you with a better life, and therefore change must be made, and in order for change to take place, you must go down to the street. People take to the streets for very legitimate demands, such as overthrowing a government or demanding a change of president, and then you find some element taking the crowds to hit the infrastructure to hit civilian targets so that the process is the destruction of the state, and thus hijacked the change to its advantage (47). for this? The generation of wars is survival and achieving its goals, or will time advance to the fifth generation (48).

The second topic: the sources and forms of cyber threats to global security

The first requirement: cybercrime

First: criminal groups

The Internet is a double-edged sword, as it performs great and great services for countries, commercial, industrial and scientific establishments, and consumers all over the world. Any country, group, company, or individual can create a website for himself on this network, and he can access it regardless of their homelands, beliefs, or Their intellectual tendencies, treat everyone equally, make people in this universe tend to form a single global community in which any individual can enter this network, and roam the world without borders, restrictions, or oversight, and this great and rapid development of the Internet, what you would have known for its first appearance, This network and its use for a lot of crimes, and it helped inter alia.

The Seybold Report
ISSN 1533-9211

Third: Cases of confrontation at the international level:

There were many cases of cyber confrontation at the international level, but it did not reach the stage of war, as it played a prominent role in influencing the relations of state actors with each other, in addition to the effects it produced predicting the possibility of expanding the scope of cyber-attacks in the future. In recent years, offensive cyber tools have appeared. As an attractive tool for countries to achieve their interests, whether by using them alone or as part of military operations on a large scale, and despite the difficulty of counting all electronic attacks that occur in the world, but in a study on cyber (electronic) conflicts, Brandon Valeriano Brandon Valeriano and Ryan C Mannes collected accurate data on electronic confrontations around the world in the period from 2001 to 2011. The authors sought through this study to try to limit the cyber-attacks (electronic) launched by countries against others and information spread confirming their occurrence.

Cyber-attacks without the government officially announcing them, which means that they cannot be counted. The following table presents the results reached by the two authors, which show the number of cyber-attacks that occurred between countries with a conflict or cyber confrontations between them, according to the published information and analysis of those attacks However, it is noted here that there is no definitive mechanism through which certain cyber-attacks can be attributed to countries that have not explicitly announced that, which often does not happen. (53).

The second requirement: cyber-attacks against state and non-state actors

First: Cyber Attacks Against State Actors:

1- The cyber-attack on Estonia in 2007:

announced the government. According to the “e-Estonia” plan, it will transform it into an electronic state and an “electronic society” in the sense that all government and banking work is done without paperwork. Even voting in elections takes place over the Internet. The country of 1.3 million people was the first country to make Internet connectivity a human right. In 2016, 99.6% of transactions were conducted through electronic banking services, and 96% of the population declared their income electronically (55).

Cyberattacks have become a tool of war used by both the United States of America and Iran, as a result of the ongoing tension between the two countries, which increased the frequency of cyberattacks, especially after President Donald Trump's administration imposed sanctions on the Iranian petrochemical sector earlier in June 2010. And Iran shot down an American reconnaissance plane near the Strait of Hormuz, and the United States launched electronic attacks targeting Iranian computer systems used to launch missiles, and an Iranian spy network, after Iran shot down a drone belonging to the United States of America, and after this incident, Washington accused Tehran of escalating in cyber-attacks. The director of the National Security Agency, Chris Kreese, said that officials detected an increase in malicious electronic activity directed at the United States by people

The Seybold Report
ISSN 1533-9211

Second: Cyber-attacks against non-state actors

1- Cyberwar between Israel and non-state actors:

In July 2006, Hezbollah killed six Israeli soldiers and kidnapped two in border raids. The Israeli response destroyed Lebanon's infrastructure and claimed the lives of more than a thousand civilians. The conflict lasted about a month until it ended with United Nations Resolution No. (1701), and the military operations were accompanied by other electronic operations on both sides. The website of Al-Manar channel, affiliated with Hezbollah, was subjected to distributed denial-of-service attacks that analysts linked between it and Israel. Reports were also issued. It was confirmed that hackers affiliated with Hezbollah were able to control the networks of the Israel Defense Forces located on the border with Lebanon for intelligence purposes. This war was of great importance because it witnessed a combination of traditional, electronic and informational operations. Hezbollah has used cyberspace to discuss the opinions of armies and peoples and their actions in certain crises, by using their website to publish news to the world about events in various languages, including Hebrew, in a way that serves their interests. Also, Israel's closing of Hezbollah's websites is similar to what Russia did by closing Georgian websites in 2008. What is different in this case is that Hezbollah's response, and doing so in the light of large-scale information operations, just as the IP address hijacking operations A number of Israeli websites have enabled Hezbollah to continue to spread strategic messages to the outside world (71).

The third topic: cyberspace in the American strategic perception

The first requirement: cyber deterrence and global security management

Deterrence in the past began traditionally in its powers and tools and was dependent on the usual means of fighting, and on the threat of using conventional weapons. Therefore, the opponent was promised a painful punitive strike in the event of an attack by him, and this is what was called punitive deterrence, and nuclear deterrence was limited to threatening to use nuclear weapons Whether this use is partial or complete, limited or comprehensive (73).

And we can say that deterrence depends on the threat of using military force, without actually using it, with the aim of intimidating the opponent and subjugating him, and instilling in him the conviction of the ability to exact retribution from him without turning the intention into an act that harms him, and this is the boundary between the use of the threat of force and its actual use. Which constitutes the meaning of deterrence and its being (74)?

First: Establishing cyber armies or councils:

The escalation of international interest in cyberspace, especially after it provided new tools and mechanisms as a means and a mediator to threaten the work of vital facilities and the global infrastructure of information, and its non-stop in front of the sovereignty of the state, which made it a fertile environment for non-peaceful use by all the various actors who ranged between using states to non-state actors, and this appears in the use of cyberspace as an arena for cold war, psychological warfare and ideas, or through using it to wage wars and terrorism between states or the use of individuals or terrorist groups, or piracy or organized crime in a way that

The Seybold Report
ISSN 1533-9211

affects the civilian nature, or peaceful cyberspace," and several reports confirm the significant increase in the frequency of cyberwar attacks between some countries, which are carried out by groups supported by several governments, and these wars are now targeting vital sectors, such as nuclear facilities, infrastructure, electricity, oil and gas companies, as well as banks, and the targets range From stealing sensitive data, causing financial terror to victims, and even vandalism (80).

Many countries have established councils and cyber armies, where some governments, such as the United States of America, China and Russia, have found that these cyber armies are a means to achieve the strategic goals of the country, and the most important attempt to penetrate the electronic systems of other countries, and steal data, information, and military and strategic plans, and there An increasing trend among countries to establish cyber units or cyber councils, the most prominent of which are: The security consulting agency Zigorion Consulting in Information Analysis confirmed that there are five major countries in cyber security that have increased funding for defense cyber capabilities after a series of American and Israeli cyber-attacks on Iranian nuclear sites in 2010 Analytics are based on the opinions of experts and officials, background information from international organizations, and more. This analysis is based on data from published sources," said Vladimir Ulyanov, director of the Analytical Department at the Zikuryon Agency. The company does not publish information about funding and the number of employees of the Cyber Army. "Moscow is investing heavily in information defense systems and we now have a leading Internet power," Ulyanov emphasized. According to Ulyanov, the United States spends more on cybersecurity than any other country. The Department of Defense has an annual budget of seven billion dollars for cybersecurity and a hacker staff of more than nine thousand. After the United States each China and the United Kingdom spend one and a half annually One billion and four hundred and fifty million dollars, respectively. "On average, about 1% of North Korea's military budget is allocated to cybersecurity, but nearly 20% of defense resources are allocated to this purpose," Ulyanov added. In the world, according to the report, the Russian cyber security forces have reached a thousand employees, and the Russian Ministry of Defense spends about three hundred million dollars annually on such activities (81).

1- The United States Cyber Army:

The United States relies in cyberwars on six elements, which is the American unit of the "Cyberspace Command", which is specialized in planning, coordinating and managing cyberwarfare operations, with the rest of the branches that follow it, and a cyber-army unit affiliated with the American unit of the Cyber Army Command, and receives its orders from it, and it consists Of three smaller units, there is also the Cyber Unit with the Marine Force, which specializes in protecting and securing Marine facilities from cyber-attacks, and there is also a cyber-army unit, the Navy, and it works similarly to its predecessor, but for US naval facilities in addition to all information about cyber wars, and the fifth unit is Air Force 24, which specializes in aviation and the US Air Force, and three wings branch out from it, and the sixth unit is the US Tenth Fleet, which It performs intelligence missions for the US Navy and was originally established to coordinate between the US Navy forces in World War II.

The Seybold Report
ISSN 1533-9211

US President Donald Trump has officially approved a new military body specialized in space called the "US Space Force", and this is the first military force to be established in the country in more than seventy years, and it falls within the US Air Force. Near Washington, space as the newest battleground in the world (82).

2- Russian Cyber Forces:

A spokesman for the Russian Ministry of Defense, (Igor Yegorov), said that Russia plans to build a comprehensive electronic system in stages to be completed in 2017 to protect the infrastructure of the armed forces from electronic attacks, as Defense Minister (Sergei Shoigu) ordered, last summer, to list five hundred Distinguished students in the use of computers in scientific units.

3- China - Unit 61398:

It is a secret unit of the Chinese People's Liberation Army, which carries out electronic espionage operations and steals economic information, especially from the United States of America. It began launching its first attacks since 2006, and stole hundreds of terabytes of private data for one hundred and forty-one organizations, including technology blueprints, manufacturing processes, data, documents, pricing and marketing plans, emails and contact lists, and it was also noted that no less than fifteen of these companies It is located in the United States of America, and it is believed that Unit 61398 is under the management of the Second Office of the Third Department of the People's Liberation Army Staff, and it is located in the Shanghai region. From industrial and government institutions, around the world since at least 2006, and Unit 61398 relies on a network of Chinese electronic hackers in thirteen countries, most of which are located in the United States that includes more than a hundred computers

4- The Canadian Army:

One of the military forces that focused on developing its cyber capabilities at a time when Canada deals with the military doctrine that believes in the growing role of electronic operations in modern warfare. the threats expected from them. The Canadian Armed Forces have invested heavily in technologies that radically increase the speed and accuracy of modern military operations, drawing on the highly complex domain of cyber to fulfill their primary responsibilities for the defense of Canada. Canada trains its soldiers on cyber missions that include temporarily shutting down websites, or spreading false information over the Internet, which evolves into dangerous and sophisticated attacks against real targ

5- Israeli Cyber Forces: Unit 8200

It is the unit responsible for commanding cyber warfare in the Israeli army, which was established in 1952 and which forms an alliance with the US National Security Agency (NSA) and the US Cyber Command. Asia, Africa and Europe, and this force has played a major role in striking the Iranian nuclear program through determination and experience."

The Stuxnet virus, which infected 1,000 Iranian centrifuges and disrupted the nuclear program, indicates that the role played by Unit 8200 of the Israeli Military Intelligence Division is the second largest installation force in the world, after the United States.

The Seybold Report
ISSN 1533-9211

6- North Korean Cyber Forces - Office 121 in North Korea:

“North Korea has a special unit for cyberwarfare, which is Bureau 121, and its main targets are South Korea, the United States and Japan, and it was established in 1998, and according to cyberwarfare experts around the world, the bureau was not famous for huge operations. It was responsible for the Sony breaches that caused millions of losses. And made the company's employees return to using paper and pen to complete their work, and it is believed that the number of office personnel exceeds one thousand and eight hundred people, and the South Korean Ministry of Defense said that the electronic piracy army in the North Korean armed forces increased its number to six thousand soldiers, or double the estimates of 2013.

7- The German Cyber Army:

"The first explorer computer in the world was (Colossus), its goal was to discover the German army's codes, so the Germans believed that since that time they were being targeted, but now Germany has an electronic army in addition to its land, sea and air forces, as the German Minister of Defense (Urzo Lavon der Leyen announced in Bonn), About the start of the work of the electronic army as an independent weapon within the traditional German army"(82).

8- Iranian cyber force

Iran was not far from the battle of cybersecurity, and it is one of the countries that formed a cyber-army at an early date, and formed a force called (Parasto) (). It is formally related to the government of Iran, but does not officially recognize its subordination to it, and this force declared its loyalty to the Iranian Supreme Leader, and according to successive media reports, "the Iranian Revolutionary Guard developed plans to form a cyber-army in 2005, under the leadership of Muhammad Hossein Tajik, Until his assassination took place, and on the other hand, the hidden Iranian electronic group has repeatedly claimed responsibility (85).

Second: Cyber Weapons:

1- Definition of cyber weapons:

"It is malware that works for military, paramilitary, or intelligence purposes. You will not see these weapons, you will not hear a sound, and you will not smell the burning gunpowder for them, but if the enemy succeeds in targeting you, its planes will burn everything, according to one of the American officers who specialize in war." Cyber and non-lethal weapons, electronic warfare relies on the use of high energy, radio waves and laser beams, to confuse or paralyze the (88).

CONCLUSION

As cyber security is considered one of the most important areas of security in the twenty-first century, and it is known that cyber domination draws the features of wars in the next century, which necessitates a change of strategy in the direction of escalation with other hostile forces active in the arena of cyber war that has been fought over for more than ten years by teams of Special forces of major countries and groups of mercenary hackers recruited as necessary. And what is meant by cyber warfare are operations in cyberspace that use means and methods of

The Seybold Report
ISSN 1533-9211

fighting that amount to the level of armed conflict or are conducted in its context, within the intended meaning of international humanitarian law. Concerns arise due to the vulnerability of electronic networks and the potential human cost of cyber-attacks. When a country's computers or networks are attacked, hacked, or disrupted, civilians are at risk of being deprived of basic needs such as drinking water, medical care, electricity, and more.

Cyberwarfare has emerged as a tool of the fifth generation of warfare, and if the goal of the American special forces for cyberwarfare lies in repelling attacks from hostile cyber teams, it also worked to penetrate the social networking sites of ISIS, which contributed to obscuring broadcast channels active in recruiting potential terrorists.

References

1) Alex Michael, Cyber Probing: The Politicisation of Virtual Attack, Defense Academy of the United Kingdom, September 2010, p.68.
2) Emile Amin, Global Cybersecurity... Background Wars and Terrorist Spaces, INDEPENDENT Arabic, 2020, available at the following link.
https://www.independentarabia.com/node/93586/%D8%B3%D9%8A%D8%A7%D8%B3%D8%
3) Nisreen Al-Sabahi, Cyber Wars and Global Security Challenges, Arab Center for Research and Studies, available at the following link http://www.acrseg.org/40594.
4) Dhiab Al-Badaina, Security and Information Wars, Dar Al-Shorouk for Publishing and Distribution, 2002, p. 207.
5) Ali Hussein Bakir, The Fifth Domain.. Electronic Wars in the 21st Century, previous reference.
6) Alex Michael, "Cyber Probing: The Politicisation of Virtual Attack", Defense Academy of the United Kingdom, September 2010, p. 1.
7) Cyber War, "The Next Threat to National Security and What to Do About It", by Richard A. Clarke and Robert Knake, Harpercollins e-books, New York, 2010.
8) Richard A. Clarke and Robert Knake, Harper Cyber War, "The Next Threat to National Security and What to Do About It", collins e-books, New York, 2010. (Omar Hamed Shukr, Cyberspace, the Fifth Domain, Political Science and International Relations website, 2019, available at the following link: https://www.elsiyasa-online.com.
9) Nabil Farouk, You are the army of your enemy, Al-Nahda Publishing Group: Egypt, 2016, p.4.
10) Tokyo, 70 Concerning the American attack with the nuclear bomb on Japan, Harry Truman tried to justify the bloody decision at length, Akhbar Al-Khaleej Newspaper, Issue 11313, 20 / August / 2015.
11) Syed Abd al-Nabi Muhammad, The Conflict of Nations and Fifth Generation Wars, Arab Press Agency, 2019, pg. 313. ((Mustafa Ahmed, The Fourth Generation of Wars: The Global Conspiracy: The Modern Application of The Protocols of the Elders of Zion, Al-Manhal e-books, 2017, p. 6.
12) Ehab Khalifa, Social Media Wars, Al-Araby for Publishing and Distribution, 2016, p. 75.
13) Majdi Kamel, Wars of the Fourth Generation, (Wars by proxy), Dar Al-Kitab Al-Arabi, 2016, pp. 88-90.
14) Khaled Azab, "Fifth Generation Wars": Communication Networks and Electronic Recruitment, Al-Hayat website, August 19, 2018. Available at the following link, http://www.alhayat.com/article/4598761.
15) America resorts to fifth-generation warfare to drain Iran, Al-Watan Online, Sunday, June 23, 2019, https://www.alwatan.com.
16) America resorts to fifth-generation warfare to drain Iran, Al-Watan Online, Sunday, June 23, 2019, https://www.alwatan.com.

The Seybold Report
ISSN 1533-9211

17) Adel Abdel-Sadiq, Future Wars... The electronic attack on Iran's nuclear program, International Policy Journal, Al-Ahram Foundation, April 2011.

18) Adel Abdel Sadiq, Electronic Terrorism: Power in International Relations: A New Style and Various Challenges, Cairo: Center for Political and Strategic Studies, first edition, 2009, p. 155, p. 229.

19) Richard K. Betts, Confident after the cold war: Arguments on Causes of War and Peace, 2nd, New York: Longman, 2002, p557.

20) Sovereignty, cyber warfare, the dreadful war of the future, Arab Forum for Defense and Armament, 2019, available at the following link. https://defense-arab.com/vb/threads/130964/page-4

21) Jennie M.Williamson, Information Operations: Computer Network Attack in the 21st century, Strategy Research Project (Pennsylvania: U.S. Army War College, Carlisle Barracks, 2002, 15-22).

22) The German Marshall Fund (GMF) - United States works to enhance transatlantic cooperation in order to deal with regional, national and global challenges and opportunities in the spirit of the Marshall Plan: an economic plan launched at the initiative of former US Secretary of State George Marshall, in 1947, from In order to help European countries to rebuild what was destroyed by World War II.

23) Christina Kosch, Senior Resident Researcher at the German Marshall Fund (GMF) USA, published by Adel Rafik, Egyptian Institute for Studies, 2018, p. 1, https://eipss-eg.org

24) Bohn, Dieter, US Cyberattack Reportedly Hit Iranian Targets, The Verge, June 22nd 2019, Accessed on July 14th 2019, Available At: https://www.theverge.com/2019/6/22/18714010/us-cyberattack -iranian-targets-missile-command-report.

25) Christina Kosch, previous source, p. 6.

26) Mostafa Alawi, The Concept of Security in the Post-Cold War Phase, in the papers of the conference held by the Center for Asian Studies May 4-5, 2002: Security Issues in Asia, edited by: Hoda Mitkees, and Mr. Sidqi Abdeen (Cairo: Faculty of Economics and Political Science, Center Asian Studies, 2004, p. 14.

Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare (New York: Cambridge University Press, 2007): 1-14.

27) Morgane Fouch, Robert Macrae and Jon Danielsson, “Could a Cyber Attack Cause a Financial Crisis,” World Economic Forum (13 June 2016), online e-article, https://www.weforum.org/agenda/06/2016 /could-a-cyber-attack-cause-a-financial-crisis

28) Arsenio T. Gumahad, Cyber Troops and Net War: The Profession of Arms in the Information Age (Alabama: Air University. Air War College, 1996): 57-156.

29) Myriam Dunn, The Cyberspace Dimension in Armed Conflict: Approaching a Complex lssue with Assistance of the Morphological Method, Information and Security: An International Hournal 7, 2001, 14, online e-article, http://procon.bg/system/ files/07.08_Dunn.pdf

30) Jennie M. Williamson, Information operation, op. city, pp15-22.

31) Adel Abdel Sadiq, First Edition / Electronic Terrorism: Power in International Relations: A New Pattern and Various Challenges, First Edition, Al-Ahram Center for Political and Strategic Studies, 2009, p. 49.

32) Cyberwar and its repercussions on global security, Algerian Encyclopedia of Strategic Studies and Policies, 2019, available at the following link:

https://www.politics-dz.com/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8

33) Miriam Dunn, Conflict of the Information Age, a published research study of the information revolution and the changing operating environment in the Research Center for Security Policy and Conflict Analysis, Germany, 2002, pp. 16-17. file:///C:/Users/DISCOV~1/AppData/Local/Temp/ZB_64.pdf

34) Adel Abdel Sadiq, Electronic Terrorism, Power in International Relations, A New Pattern and Various Challenges, first edition, Al-Ahram Center for Political and Strategic Studies, 2009, p. 155.

The Seybold Report
ISSN 1533-9211

35) British Defense Secretary Michael Fallon, Britain can launch electronic attacks to defend itself against Russia, Telecraf website, 2017, available at the following link.

https://translate.google.com/translate?hl=en&sl=en&u=https

36) Saudi Arabia warns on cyber defense as Shamoon resurfaces, Technology News, Reuters, Mon Jan 23, 2017, http://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR

37) Florian Bieber, "Cyber war or Sideshow The Internet and the Balkan Wars", Current History 99, no. 635 (Mar 2000): 124-128, online e-article, http://search.proquest.com/docview/200751259accountid=7180

38) William.J.Broad, John Markoff and David E. Sanger, Israeli Test on Worm Called Crucial in Iran nuclear delay, the new york times 15 jan 2011, online article http://www.nytimes.com/16/01 /2011/world/middleeast/16stuxnet.html_r=1&pagewanted=all

39) Adel Abdel-Razzaq, Cyberspace and International Relations: A Study in Theory and Practice, Cairo: Academic Library, 2016, pp. 22-26.

40) David Held et., Global Transformations: Politics, Economics, and Culture California: Stanford University press, 1999.

41) Joseph. S.Nye. The future of power, New York: Public Affairs, 2011, 24.

42) E.Nakashima, U.S. Accelerating cyber weapon Research, the Washington post, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html.

43) Adel Abdel Sadiq, Electronic Power: Weapons of Mass Proliferation in the Age of Cyberspace, Al-Seyassah Al-Dawla Magazine, Issue 188, April 2012.

44) Omar Hamid Shukr, Cyberspace, the Fifth Domain, Political Science and International Relations website, 2019, available at the following link: https://www.elsiyasa-online.com/.

45) Syed Abd al-Nabi Muhammad, The Conflict of Nations and Fifth Generation Wars, Arab Press Agency, 2019, pg. 313.

46) Ehab Khalifa, Social Media Wars, Al-Araby for Publishing and Distribution, 2016, p. 75.

47) Majdi Kamel, Fourth Generation Wars, (War by proxy), Dar Al-Kitab Al-Arabi, 2016, pp. 88-90.

48) Ghada Nassar, Terrorism and Cybercrime, Cairo: Al-Qasr Al-Arabi Street, 2017, p. 14.

49) Ghada Nassar, Terrorism and Cybercrime, previous source, p. 14.

50) Omar Musa al-Fiqi, Information Crimes and Computer and Internet Crimes: In Egypt and the Arab Countries, Cairo: Modern University Office, 2006, pp. 96-97.

51) Muhammad Hossam and Mahmoud Lotfi, Legal Protection for Electronic Computer Programs, Cairo: Culture Jar for Printing and Publishing, 1987, p. 7.

52) Ahmed Hossam Taha Tammam, Crimes Resulting from the Use, Criminal Protection of Computers, unpublished PhD thesis, Tanta University: Faculty of Law, 2000, pp. 110-111.

53) Aref Khalil Abu Eid, Internet Crimes, a comparative study, University of Sharjah Journal of Sharia and Legal Sciences, Volume 5, Number 3, 2008.

54) Brandon Valeriano Ryan cmaness, the dynamics of cyber conflict between rival antagonists, journal of peace research, pp347.

55) Brandon Valeriano and Ryan C Maness, The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011, Journal of Peace Research, vol.51, no.3, pp:347-360.

56) Brandon Valeriano and Ryan C Maness, The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011, Journal of Peace Research, vol.51, no.3, pp: 347-360. Political Editor, Russian piracy is not new, the first electronic war in Estonia, the magazine's website, 2017, available at the following link:

The Seybold Report
ISSN 1533-9211

https://arb.majalla.com/2017/03/article55257690/%D8%A7%D9%84%D9%82%D8%B1.

57) Russia accused of unleashing cyberwar to disable Estonia, 2007 Available at the following link https://www.theguardian.com/world/2007/may/17/topstories3. russia,

58) Nouran Shafiq, International Politics and Strategy, Electronic Threats to International Relations, Cairo: The Arab Bureau of Knowledge, Heliopolis: 2016, p. 139.

59) Nuran Shafiq, previous sourcee, p. 136.

60) Eneken Tikk, al International Cyber Incidents: Legal Considerations. CCD COE Publications. (2010). p16.

61) Ahmed Awad, the story of "Cyber Wars": A global battle without weapons that interferes with the results of the presidential elections, Al-Masrya Al-Youm website, January 10, 2018, available at the following link: https://lite.almasryalyoum.com/box/177468/ .

62) Heather A. Conley et al. (August, 2011). Russian Soft Power in the 21st Century: An Examination of RUSSIAN Compatriot Policy in Estonia. Center for Strategic and International Studies. p6

63) Heather A. Conley et al. (August, 2011). Russian Soft Power in the 21st Century: An Examination of RUSSIAN Compatriot Policy in Estonia. Center for Strategic and International Studies. p6

64) Sin-seok Seo et al. (October, 2011)

65) The secret revenge between Iran and America, Sky news Arabia, Abu Dhabi 2019, available at the following link, https://www.skynewsarabia.com/technology/1261693-%D8%.

66) Richard A.Clarke and Robert K. Knake. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins Publisher.pp147-149

67) Ziyad Abd al-Rahman Ali al-Kourani, A geostrategic vision for the future of regional conflicts in the area of competing strategies, al-Manhal, 1018, p. 155.

68) Nuran Shafiq, The Impact of Electronic Threats, previous source, 153.

69) Paulo Shakarian et al. (2013). Introduction to Cyber Warfare: A Mu;tidisciplinary Approach. Syngress. p27.

70) Nicole Perlroth. (October 23, 2013). Sees Iran Firing Back. The New York Times, URL: http://www.nytimes.come/2012/10/24/ business/global/cyberrattack-on-saudi-oil-firm-disquets March 7, 2014.

71) Rono Tertre, Nuclear Weapons Between Deterrence and Danger, Translated by: Abd al-Hadi al-Idrisi, United Arab Emirates: Abu Dhabi Authority for Culture and Heritage (Kalima), 2011, p. 43-47

72) Abdul Qadir Muhammad Fahmy, reference previously mentioned, p. 115-117

73) James J. Wirtz (eds.), Complex Deterrence Strategy in the Global Age. United States: the University of Chicago Press, 2009, p. 5.

74) Michael Krepon, Space and Nuclear Deterrence, In: Michael Krepon & Julia Thompson (Eds.), Anti-Satellite Weapons Deterrence and Sino-American Space Relations, United States: Stimson Center, September 2013, p. 15

75) Oceana, Jerome Orji, Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States, Defense of Terrorism Review, Vol. 6, No. 1 Spring and Fall 2004, pp. 31-46. https://democraticac.de/?p=43837

76) The Approaches and Limitations of Cyber Deterrence, Introduction to Computer Security, Fall 2005, p. 1-11.

77) Kevin R. Baker, Strategic Deterrence in Cyberspace: Practical Application, Graduate Research Project Submitted to the College of Electrical and Computer Engineering Graduate School of Engineering and Management, Air Force Institute of Air Force Education and Training Technology in Partial Implementation of Master's Degree Requirements in Cyber Warfare, 2009, p. 7; Report on Cyber Deterrence Policy, available at: http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/

The Seybold Report
ISSN 1533-9211

78) Cyber deterrence and cyberwar, Rand Corporation, 2009, p31. Martin C. Libicki,

79) Sico van Der Meer & Franc Paul Van Der Pulten, U.S. Deterrence against Chinese Cyber Espionage the Danger of Proliferating Covert Cyber Operations Nether Lands Institute of International Relations, September 2015, pp. 1-7.

80) Sico Van Der Meer & Franc Paul Van Der Pulten, Op.cit, pp. 1-7.

81) Charles L. Glaser, Deterrence of Cyber Attacks and U.S. National Security, Report GW-CSPRI, June 2011, p. 5.

82) Wael Lababidi, A close link between geopolitical tensions and cyber attacks, Economic Statement, UAE, December 29, 2019, available at the following link,

https://www.albayan.ae/economy/local-market/2019-12-29-1.3738629.

83) Katehon Research Center, What are the five best electronic armies in the world and what is the ranking of the Russian cyber army, 3/1/2017, can be viewed at the link, https://katehon.com/ar/article/mhy-fdl-khms-jywsh- lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy seen on 9/13/2019.

84) Khaled Al-Tharwani, Virtual Armies between the International Conflict and the Local Political Settlement, Al-Nabaa Informatics Network, Saturday 25 June 2017, at the following link,

https://annabaa.org/arabic/informatics/11558.

85) Trump officially announces the formation of the Space Forces, BBC Arabic, December 21, 2019, available at the following link: https://www.bbc.com/arabic/science-and-tech-50878479

86) Ehab Khalifeh, A New Pattern of Jobs in Military Institutions, The Future for Advanced Studies and Research, 2015, available at the following link,

https://futureuae.com/en-/Mainpage/Item/445/%D8%A7%D9%84%D9%88%D8

87) Adel Abdel Sadiq, Patterns of (cyber warfare) and their repercussions on global security, published in Hurriyat on 03-07-2017, at the following link, https://www.sudaress.com/hurriyat/225278

88) Ehab Khalifa, Electronic Power, pg. 96.

89) North Korea raises the number of its electronic piracy army to 6000, Akhbar Al-Youm electronic portal newspaper, Wednesday, January 07, 2015, available at the following link

https://akhbarelyom.com/news/newdetails/296897/1/%D9%8.

90) Mike Mali, translated by Salah Hazeen, Electronic Minds, Beirut: The Arab Institute for Studies and Publishing, 2008, p. 151.

91) Sputnik Arabic website, Cyber DefenseGerman Ni was aware of breaches of personal data of politicians, published on 5/1/2019, available at the following link: https://sptnkne.ws/v7ua.

92) Made for Minde, Germany launches its electronic army and defines its exact tasks, 2017, available at the following link, https://p.dw.com/p/2alSy.

93) Mahdi Mubarak Abdullah, The Iranian Cyber Army, The Secret Destructive Force, Ajrasah Woman of Truth website, 2019, available at the following link. http://www.gerasanews.com/article/325741.

94) London - Reuters, August 30, 2018, last updated on August 29, 2018.

95) America accuses Iran of launching electronic attacks on banks and a dam in New York, Washington - Reuters, March 24, 2016, available at the following link

https://arabi21.com/story/897099/%D8%A3%D9%85%D8%B1%D9 .

96) Mahdi Mubarak Abdullah, The Iranian Cyber Army, the Destructive Secret Force, Gerasa website 4/22/2019, available at the following link http://www.gerasanews.com/article/325741 on 9/13/2019.

The Seybold Report
ISSN 1533-9211

97) Nabil Al-Atoum, The Iranian Electronic Army, published research: Umayya Center for Research and Strategic Studies - Dar Ammar for Publishing and Distribution, 2015, p. 9. http://www.umayya.org/acrpsbooks/8123

98) Salih Hamid, "Al-Arabiya.net" reveals the secrets and activities of Iran's electronic army, 15/January/2017, available at the following link, https://www.alarabiya.net/ar/iran/2017/01/15/.

99) An "invisible" weapon that completely paralyzes armies. Get to know it, Marib Press Agencies, 2019, available at the following link, https://marebpress.org/news_details.php?lang=arabic&sid=156003&utm_campaign=nabdapp.com&utm_medium=referral&utm_source= nabdapp.com&ocid=Nabd_App

100) Military electronic warfare is an "invisible" weapon that completely paralyzes armies, Sputnik Arabic, 2020, seen on 1/24/2020 at the following link https://arabic.sputniknews.com/military/

101) Powerful 'Flame' Cyberweapon Torching Mideast Computers: Discovery News". News.discovery.com. 2012-05-30. http://news.discovery.com/tech/flame-cyberweapon-120530.html. Retrieved 2012- 12-07.

102) Military Wiki, the largest free interactive military encyclopedia on the Internet in the world, cyber weapons, 2014, seen on 9/1/202 at the following link. https://military.wikia.org/wiki/Cyberweapon#cite_note-4

103) Security affairs ,Cyber Weapons, April 3,2012, Was seen 20/1/2020, On the followinglink.http://securityaffairs.co/wordpress/3896/intelligence/cyber-weapons.html .

104) Ehab Khalifa, Electronic Force, previous source, p. 83.)) Stallings, William (2012). Computer security: principles and practice. Boston: Pearson. p. 182. (Ludwig, Mark (1998). The giant black book of computer viruses. Show Low, Ariz: American Eagle.

105) Dezad Kalashnikov Blog: The World of Weapons, A Supernatural Weapon That Can Disable All Electronics With The Push Of A Button, 2013, available at the following link, https://dzkalashnikov.blogspot.com/2013/10/supernatural-weapon-that-can-disable.html On 9/11/2019.

106) Spymaster sees Israel as world cyberwar leader, 15 December 2009 http://www.circleid.com/posts/spymaster_sees_israel_as_world_cyberwar_leader/ .

107) Record 54.5 billion cyber-attacks detected in Japan last year, The Japan Times, FEB 21, 2016, https://www.japantimes.co.jp/news/2016/02/21/national/crime-legal/record -54-5

108) America extends its cyber security umbrella to protect Japan, Al Arab Qatari newspaper, May 30, 2015.

109) History of Cyber Attacks, Timeline, NATO Review, 2013.

htt97ps://www.nato.int/docu/review/2013/Cyber/timeline/AR/index.htm

110) CHOE SANG-HUN," Computer Networks in South Korea Are Paralyzed in Cyber-attacks, The New York Times, March 20, 2013. https://www.nytimes.com/2013/03/21/world/asia/ south-korea-computer-network-crashes.html

111) An attack on websites in South Korea, BBC Arabic, June 25, 2013. The link was last visited on August 2, 2016.