جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
أوراق السياسات الأمنية
https://nauss.edu.sa/
Security Policy Papers
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

تهديدات الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية

Arab Region Security Threats in the Fifth Domain: Towards a Strategy for Protection

إيهاب خليفة
مركز المستقبل للأبحاث والدراسات المتقدمة
الإمارات العربية المتحدة

Ehab Khalifa
Head of Monitoring Technological Developments Unit
the Future Center for Advanced Research and Studies

Key outputs:

- A unified Arab vision shall be established, in addition to establishing a strategy that is capable of handling cyber-attacks as it threatens the security of the region. Arab countries shall operate under the framework of such a strategy. This could be achieved through the Arab Interior Ministers Council.
- Emphasize the importance of the strategic cooperation between countries in the region through sharing information and data necessary for analyzing the digital evidence that assists in discovering cyber-attacks as they occur and take actions to mitigate its effects, in addition to monitoring pirated financial transactions and encrypted currencies used to finance rebel and terrorist movements.

Abstract

As the world tends to increasingly depend on smart and modern technologies and adopt models of smart governments and cities to benefit from the gains of the Fourth Industrial Revolution in enhancing the style of human life, meanwhile and during the acceleration of the technological modernization process that countries and communities experience, especially during the spread period of virus Covid-19, to guarantee the continuity of the urban human activity while adhering to the quarantine and social distancing instructions, the world has become more exposed and vulnerable to the risks of cyber threats.

Moreover, with the obvious increasing rate of cyber-attacks and the increase of its ability to destroy, cyber-attacks have become capable of destroying nuclear reactors and satellites in

addition to destroying critical infrastructures, hence, cyber warfare has become more probable than before in a way that could be more brutal than any other war; within a few minutes, thousands of people might be killed if a successful cyber-attack targeted one of the vital facilities in a country such as aviation systems or hospitals.

Cyberspace is considered the main battlefield for such cyber armies, although it is not the only one, similar to the armed forces where they fight in the four traditional domains (land, sea, air, and outer space) cyber armies fight in all these domains combined in addition to fighting also in the fifth virtual domain which is cyberspace.

Therefore, this research is important as it discusses Arab region security threats in the fifth domain, these new threats are resulting from the increasing dependency on cyberspace. This research strives to provide a vision that assists decision-makers in drafting an Arab National Strategy to face the risks of cyber threats that challenge the Arab regional cyber security. It consists of three main elements, the next battlefield, appropriate weapons, and fighting armies. The battlefield will be a cyber one, the weapons will be programmed, and the armies will operate from behind the screens.

Introduction

As the world tends to increasingly depend on smart and modern technologies and adopt models of smart governments and cities to benefit from the gains of the Fourth Industrial Revolution in enhancing the style of human life, meanwhile and during the acceleration of the technological modernization process that countries and communities experience, especially during the spread period of virus Covid-19, to guarantee the continuity of the urban human activity while adhering to the quarantine and social distancing instructions, the world has become more exposed and vulnerable to the risks of cyber threats; the reason behind this is that the more we depend on the internet to manage our daily life affairs the more the targets that attract the pirates varies, hence the chances of facing breaches and cyber-attacks increase.

Moreover, with the obvious increasing rate of cyber-attacks and the increase of its ability to destroy, cyber-attacks have become capable of destroying nuclear reactors and satellites in addition to destroying critical infrastructures of power and fuel stations, communication systems, transportation systems, hospitals, and so on. Therefore, this means that cyber warfare has become more probable than before in a way that could be more brutal than any other war; within a few minutes thousands of people might be killed if a successful cyber-attack targeted one of the vital facilities in a country such as aviation systems or hospitals.

Cyberspace is considered the main battlefield for such cyber armies, although it is not the only one, similar to the armed forces where they fight in the four traditional domains (land, sea, air, and outer space) cyber armies fight in all these domains

combined in addition to fighting also in the fifth virtual domain which is cyberspace.

Whereas the appropriate weapon to achieve deterrence and maintain security must be a derivative from its own age, this is a condition so it could be effective and appropriate, the weapon here must be a cyber and smart one, a different weapon from other traditional ones. For example, when the human community was agricultural the weapons were pikes, spears, and swords, which were all weapons made directly from land resources with minor human intervention. During such era, man has taken more control over nature and later one transformed into an industrial community that is capable of developing tanks, planes, and other weapons. Whenever the community transforms into a "Smart" one then the weapon must go along with this new age, otherwise, it will not be effective in maintaining the security of the country or its goals.

Therefore, this research is important as it discusses Arab region security threats in the fifth domain, these new threats are resulting from the increasing dependency on cyberspace. The research strives to provide a vision that assists decision-makers in drafting an Arab National Strategy to face the risks of cyber threats that challenge the Arab regional cyber security. It consists of three main elements, the next battlefield, appropriate weapons, and fighting armies. The battlefield will be a cyber one, the weapons will be programmed, and the armies will operate from behind the screens.

First: The Theoretical Argument Regarding the Nature of Cyber Threats:

"Cyber Security" is considered a non-conventional element of national security, the reason behind this is that a cyberspace user can cause serious damage to the other party and paralyze his information and communication infrastructure, this may lead to serious military and economic losses, it may be done through disconnecting the communication systems between military units, fake information owned by a unit, steal confidential information about such unit, manipulate economic and financial data, fake, or delete it from computers, control an artificial intelligence system or the internet of things, or hack a flock of drones, robots, or self-driving cars and direct it to commit vandalism activities. Although the losses of such incidents are huge, the weapons used are simple; they are programs that are less than a kilobyte, represented in viruses that breach computer networks and spread fast between devices, then it starts achieving its goal in complete secrecy and high efficiency. through this process such viruses do not notice any difference between the fighter or the civilian, the public or the private, and the confidential or the known.

Definitions of cyber security vary, some describe it in a comprehensive way to express the ability to protect the country's data and networks such as: the definition of Lewis, J.A "Protecting computer networks and the information it contains from breach, damage, or malware (1)", another definition is "The ability to protect or defend the use

of cyberspace from cyber-attacks (2)", and "The art of guaranteeing the existence and continuity of the information community in a certain country, and assurance and protection of information, assets, and critical infrastructure in cyberspace (3)".

Some definitions determine the procedures and policies of cyber security, such as: the definition of the International Telecommunication Union "cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets in general (4)". Cyber Security involves reducing the risk of malicious attacks on software, computers, and networks. This includes intrusion detection tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications (5)", it is also described as "a group of technologies, processes, practices, responses, and procedures that mitigate risks, it is designed to protect networks, computers, programs, and data from attacks, malware, or unauthorized access to maintain confidentiality, integrity, and availability (6)". Also, the United States Department of the Interior defines cyber security as it is "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation (7)".

Second: Prepare for a New Generation of More Violent and Widespread Cyber-Attacks:

Cyber-attacks during the last decade were distinguished by being limited and temporary; as they did not affect a wide range of users, nor cause any paralyze to the internet or stop the governmental services significantly. Except for the military attacks such as: "Stuxnet". These attacks were limited to targeting bank accounts and hacking websites and pages on social media platforms, such attacks traditionally caused a temporary cutdown of the service, which was quickly handled by technicians and specialists.

On the contrary, since the beginning of the current decade cyber-attacks started taking a different dimension that is more developed and dangerous, driven towards this dimension by an unprecedented state of technological modernization that the countries and the region witnessed in general, especially during the spread of virus Covid-19. In this regard, the largest power stations and logistics companies around the world were targeted by ransomware. Critical infrastructures such as: dams, power stations, and hospitals became the most affected targets by the risks of cyber threats.

Therefore, it was not strange to witness an unusual summit between the President of the United States Joe Biden and the Russian President Vladimir Putin in Switzerland in June 2021, as they discussed the cyber-attacks matter as it is considered the most critical matter on the national level (8).

Accordingly, we might say that the new generation of cyber-attacks is distinguished by more complex and violent characteristics than ever before, there are several reasons behind this:

- The rapid development of cyber-attacks pattern: The pattern of cyber-attacks changes rapidly in this generation, it might be via computer devices, the internet of things, on mobile phone devices, and soon it might be via artificial intelligence systems and robots. It also might target money, political opposition, terrorism, or unjustified violence.
- Limited time gap between major attacks: The time gap between a cyber-attack and another is too short, therefore several major attacks occur during one year, it is not long before the world nearly recovers from the consequences of an attack until it faces another one that is different in mechanism, scope, and audience.
- The increase of the complexity level of an attack and its repercussions: The execution of attacks became more complicated and harder to trace or find its source. Many people from around the world participate in such attacks, in addition to the unexpected usage of devices in the hacking process, such as: drones for the purpose of deception, the repercussions for such incidents are unbearable on the level of individuals or countries.
- The prominent role of the non-state actors: Non-state actors play an important role in cyber-attacks, which might be as important as the role of states, whether they were a group of hackers, terrorist movements, international mafia, or regular individuals. Also, many hacking programs are developed in a manner that does not require a developer or specialist for its usage, but it could be bought and easily used, this opens the door for a major sector of non-specialists to participate in this type of attack.
- The increasing risk of the ransomware attack pattern: During the year in which the Coronavirus spread, the pattern of the ransomware attacks has developed and possessed a double threat. Attackers encrypt large amounts of the victims' data in order to blackmail them and take their money. After the victim pays to have his data decrypted, the hackers blackmail him once again to not leak the data. Researchers have noticed that the new generation of ransomware programs encrypts every 16 bytes of the infected file. This means that some ransomware protection solutions do not notice this matter, as "the encrypted file is statistically very similar to the original unencrypted file". This pattern is considered a new and creative encryption pattern that was not noticed before.
- Dependency on cryptocurrency: Cryptocurrency such as Bitcoin is hard to trace and does not have central management even though sale and purchase processes could be done through it. Therefore, it became the

official currency for cyber-attacks, especially ransomware attacks that have spread more than before.

As a result, cyber security companies detected during the year 2020 an unprecedented cyber state around the world. A cyber mission that targeted spying on governments and armed forces, it included more than 1093 targets in 27 countries around the world, some of which are Iran, Afghanistan, India, Pakistan, and Germany (9). In addition to that, there is an increase in the activities of national hacking groups that governments support, such as Russia, China, and North Korea, especially against the United States whether the reasons behind this is a political one related to the American elections or to impose domination and power upon Eastern Europe, or for other economical and intelligence reasons (10). On the other hand, the United States experienced a major and one of the worst security breaches of all time, it resulted in a breach of the Department of Treasury, Department of Commerce, and other Federal institutions (11). All these developments provide an indicator of the new nature of cyber-attacks that has become more violent and dangerous than before.

Third: Cyber risks and threats that affect the Arab national security:

Although many countries in the Arab region leaned towards adopting cyber security strategies and established institutions specialized in achieving national cyber security, this did not prevent the occurrence of many major cyber threats. There are several reasons behind this, from one perspective the Middle East region witnessed a significant transformation towards the expansion of digital infrastructure during the last few years. It then became an attraction point to hackers and criminal groups who take advantage of the fragile digital culture among people in the region. On the other hand, there is the regional conflict state, such as the conflict between Iran and Saudi Arabia which a part of it changed into a cyber conflict. Iran has launched several cyber-attacks towards the Saudi power sector, sometimes it affected the oil supply to international markets. Moreover, there are the activities of terrorist groups who have tried to use cyberspace for financing and recruiting purposes in the Arab region, this has made the internet one of the direct sources of threat in the Arab region.

According to the cyber security index issued by the International Telecommunication Union for the year 2020, only four Arab countries were included in the first 50 ranks of the cyber security index. They are in order: the Kingdom of Saudi Arabia which came in the second rank internationally, the United Arab Emirates came in the fifth rank, Oman came in twenty-first, Egypt came in twenty-three, Qatar came in twenty-seven (12). This index reflects the lack of regional coherence regarding cyber security, while Saudi Arabia and the United Arab Emirates came in a high rank in the field of cyber security, Oman,

Egypt, and Qatar came in an average rank, followed by the weakest countries Bahrain, Kuwait, Jordan, Lebanon, then the rest of the Arab countries.

In this regard, some risks that directly affect the Arab regional national security in the fifth domain could be defined, some of which are:

- Targeting the country's critical infrastructure: The country's infrastructure is targeted through cyber-attacks whether it was civilian or military, such as: targeting power and gas stations, financial and banking services, communication, and transportations stems. One of the examples in this regard is the cyber-attack Iran launched in 2012 against the Saudi Arabian Oil Company "Aramco", the attack resulted in the breakdown of 30 thousand computers, which made this attack the most destructive one (13). A while after, in 2016 Iran attempted another cyber-attack against computer devices in the Saudi Central Bank, Ministry of Transport, and the agency responsible for managing Saudi Airports, the attacks resulted in a loss of huge amount of data, but Saudi Agencies were able to retrieve the data from backups copies.
- Collect economic intelligence information: this could be achieved through the penetration of financial and banking databases and databases of companies and banks, then collecting information that might threaten national security. Another way is to spy on financial officials, ministers of finance, and chief executives of major companies.
- Taking control over military systems: In this regard, professional hackers or regular armies launch cyber-attacks in order to control the command-and-control system remotely. This leads to a loss of control from the command center over some weapon systems, as it might be redirected towards internal targets or friendly countries. Also, this could lead to taking control over drones, submarines deep in the sea, or military satellites in outer space hence the owner countries might lose control over them.
- Steal or manipulate military information and data: through the penetration of military databases, hackers could steal, manipulate, or digitally destroy them. In this state, cyber-attacks attempt to breach the private networks of military institutions in order to steal, destroy, or manipulate the weapon systems deployment maps, designs of military equipment, troop deployment areas, or any information related to the armed forces.
- Hack the devices of the internet of things: Devices of the internet of things and sensors are very common in smart communities, they are found inside large institutions, houses, restaurants, coffee houses, and also in the streets. This means that there is an ability to create a huge army of billions of devices that has weak security, could easily be breached,

are available everywhere, and are all connected to the internet. Hence, if these devices are hacked, controlled, and infected by viruses, worms, and trojans it will directly transform into an armed army able to destroy critical infrastructures such as banks, power stations, dams, hospitals, communication sectors, or even breakdown financial and banking services, and disable all governmental services, it could also result in the destruction of the internet itself (14).

- Controlling artificial intelligence systems: Smart communities depend on artificial intelligence technologies such as: robotics systems in factories, companies, retail stores, automated answering machines for customers, self-driving cars, and drones. If these systems are breached, we will find an army of self-driving cars around the streets killing people without knowing the real person behind it. Also, theoretically, armies of drones and robots could be controlled and redirected to accomplish killing and destruction tasks in a manner that makes the attempt of hacking these systems one of the most dangerous technological threats that humans might face (15).

Fourth: Dealing mechanisms with cyber threats on the national level:

Dealing with cyber threats requires considering its nature regarding the actors, battlefield, and the types of loss. As actors might be a state, or non-state, such as: hacking groups that participate in wars in favor of certain countries, as for the battlefield it is an artificial environment and not a natural one that is controlled by rules of nature, in addition to that, international laws can not control the interactions in such environments. This is not only a result of the absence of the sovereignty concept but because of the difficulty of identifying the real person behind launching such cyber-attacks on the other party. Losses in such events could be direct and represented in data damage, destruction of infrastructures, or destruction of military equipment, sometimes it could be indirect and represented in regression of the country's economic competitiveness and loss of trust in the national economy as a result of the cyber-attacks that target financial, commercial, and industrial institutions (16).

To be able to deal with cyber threats and mitigate its risks on the national and regional security, its special nature in the fifth domain must be recognized, which is represented in the following:

- The key role of cyberspace in managing everyday life affairs:

Cyberspace has become the center of human life, its lifeline, and source of energy and connectivity. As managing the communication and transportation systems, power stations, nuclear reactors, dams, reservoirs, controlling traffic lights, street directions, bridges, trafficking self-driving cars, drones, financial transfers, selling, and purchasing transactions are all done through technologies connected

to computer networks and internet. We can say the human life has almost left the earth, but not to mars as science fiction films introduce, but to cyberspace, in this regard, the fact of targeting a country's interest in the fifth domain is similar to announcing actual war against it, which is a case that must be recognized.

- Recognizing the cyber environment as artificial not natural one:

The fifth domain-cyberspace- is different than other traditional domains such as: earth, sea, air, and outer space. As it is an artificial domain, not a natural one, it is not governed by the laws of nature and gravity, but by data flow protocols through wires between devices and airwaves, therefore, planes, tanks, and missiles will not be useful in such a domain, and their actual value will not be worth a cent in a huge cyberwar. This fact obligates countries to strive to keep their security by developing an appropriate, efficient, and usable weapon in this new domain.

- The difficulty of depending on others to achieve cyber security:

If a country is weak or has a medium level of strength it imports weapons from major countries to achieve its military victory. This will not be useful at all in this new type of war, in contrary to a rifle held by a soldier who uses it however he desires, a foreign imported technology could be breached and remotely controlled or disabled if its manufacturer desires. This itself provides another challenge for countries, as they must develop their own weapons in such domain in order not to become a victim in case their allies decided to abandon them in favor of their enemies.

- Lack of ability to achieve deterrence in cyberspace:

Deterrence, in general, is the ability to prevent the opponent from achieving any harmful act, either because he might be afraid of a counterattack that might exceed his defensive abilities, or because of the high expenses of the attack in comparison with the gains that might be achieved (17). Nuclear deterrence is considered the classic model for understanding the deterrence act in international relations, except this model is not applicable to cyberspace, as it is characterized by the lack of geographical borders that clarifies the countries' sovereignty. Also, the weapons used in cyberspace are not predetermined and are continuously developing, they are often the result of zero-day attacks and viruses that are frequently developed, which are hard to restrict, prevent, or rationalize their usage (18). In addition to the difficulty of identifying the attacking party, or the person committing the cyber-attack in the first place, the reason behind this is the complex and interrelated nature of cyber-attacks, therefore achieving deterrence in cyberspace is not possible through the conventional concept.

Accordingly, being prepared for the next cyber battle requires the countries to put a lot of effort into the educational, developmental, and training levels. As victory in cyberspace

can not be achieved through importing all sorts of smart technologies from abroad, which could contain backdoors and bugs that could be used at any time during war. Countries that seek victory in the next battle must build their cyber weapons through their smart capabilities, without the complete dependency on importing all weapons from abroad similar to conventional weapons, in addition to establishing regional cyber alliances that contribute to achieving regional cyber security.

In this regard, maintaining national security through cyberspace requires countries to work through several main aspects: which are:

- Build national cyber capabilities:

This could be achieved by teaching children programming applications from a young age, expanding the institutions and faculties of artificial intelligence, adopting talented students in the computer field and recruiting them in the armed forces, supporting national start-ups in the field of cyber security and cyber protection, and applying legal and legislative rules that ensure maintaining a healthy cyber environment inside the country, mitigates the risks of outside cyber-attacks, apply strict standards for the critical institutions and authorities inside the country, assist financial companies and institutions in protecting their assets from any breach or leakage, and draw a limit for the misconduct of hackers, criminal organizations, and terrorist groups from manipulating the country's infrastructure.

- Develop a national cyber weapon structure:

Countries must exert all efforts in building their cyber weapon structure on their own, the weapons they use to fight through cyberspace against viruses, worms, and smart programs. In addition to, recruiting professional hackers and programmers into the armed forces in order to create cyber armies that represent a fundamental hand and contributes to achieving national security, these armies will represent "shadow soldiers" who work behind computer screens and possess the capabilities, software, and electronic technologies that enables them to change the rules of the game in times of crisis and war, so they would become pillars in managing military conflicts.

- Build regional cyber alliances:

This could be done by building new cyber alliances or developing traditional regional organizations' conventions, so they include also defending against cyber threats exactly like: NATO. This assists in exchanging information between regional security institutes regarding cyber-attacks that have a complex nature and create a regional armor that contributes to blocking cyber threats from regional neighbors.

- Create military cyber units:

Several countries around the world have turned into building cyber armies and security operations teams through cyberspace into their armed forces, they consist of information hackers whose task is to hack the computer networks of their opponents, spread spyware

and monitoring programs, execute military missions required such as breaking down the opponent's military program, take control over one of their networks, or destroy some of their electronic services, in addition to defending national networks and protecting it against any breach attempts (19).

Cyber armies' mission in times of peace is represented in providing informational and logistical support, as they spy on the enemy through hacking his network to reveal his secrets, steal the designs of advanced weapons he owns, steal his strategic and economical plans in the state of war, identifying the types of weapons he owns, places of deployment, targets he seeks to destroy in the state of war, identify troops deployment positions, revealing the number of troops he owns, and the times they sleep, their activities, the meals they eat, and also the supplier who provides such meals, each information might be useful in times of war to defeat your enemy.

In times of war, these armies are responsible for the process of defending and attacking at the same time, in addition to the task of providing support to military units fighting in different domains. The mission of attacking is executed through cyber-attacks that target the enemy's command and control systems by disabling air defense systems, disabling missile launch platforms, taking control over self-operating weapons such as drones and military robots, disconnecting communication networks between military units, in addition to executing digital manipulation and jamming the enemy's devices. On the other hand, these armies are responsible for the defense process by securing all communications between friendly military units, preventing any breach or spying attempts, ensuring secure and easy communications between fighting units, covering military forces behind enemy lines by disabling his military systems, and expose the ambushes he builds for them.

Fifth: International experience in the field of regional cooperation in fighting against cyber threats: NATO as a model:

The importance of cyberspace to NATO is not only in supporting the military operations that the alliance executes in areas of conflict, but the alliance also considers himself responsible for the safety of almost one billion individuals who represent the populations of the member countries of NATO. This support is against cyberspace threats, or modern technologies in general, such as: generation5 (G5) of communications, drones, and three dimensions printers, or against anything that might threaten the safety of either the civilians or the military. In this regard, the concept of cyber defense has become the main element of collective defense, cyberspace has taken an important position in the military doctrine of NATO.

As NATO is aware of the nature and risk of cyber threats the member countries have signed a policy for cyber defense in 2014 (NATO Policy on Cyber Defence), it has later been amended in February 2017, in order to ensure the governance of applying

such concept inside the institutions relevant to defense in NATO, and to establish a certain framework for the concept of cyber defense and incorporate it in the planning and operational processes whether it was on the civilian or military level. Hence, cyber defense has become at the center of the collective defense in NATO to protect the networks of the member countries against cyber-attacks either the attacks targeted military or civilian networks so that the members of NATO would have the right to request the enforcement of article five in the constitutive treaty if they faced a cyber-attack (20).

The concept of cyber defense for NATO includes protecting the alliance's networks against cyber-attacks and achieving cyber security of the member countries, in addition to recruiting the required cyber capabilities to assist in executing the military operations and tasks. Not only that, but NATO has also adopted the concept of Positive Cyber Defense, which means preventing an attack before its occurrence through applying preventive measures or proactive cyber-attacks, this includes attacking the source of threat to prevent possible cyber-attacks. Therefore, NATO has launched preventive cyber-attacks against some sources of threat to prevent it from launching military operations in the future against the alliance and its members.

During Warsaw Summit in 2016, NATO issued a defense authorization considering cyberspace a domain for military operations, NATO must achieve security in such a domain similar to achieving security in other conventional domains. It has considered the rules of international laws applicable in cyberspace, and the right to use force in self-defense is also applicable to cyberspace which is represented in launching cyber-attacks to protect the alliance countries. NATO has also issued "Tallinn Manual" that is considered the legal reference for NATO in cyber wars, during the same year the member countries have signed a pledge to increase their capabilities in cyber defense, NATO has devoted certain resources for education and training in the field of cyber security, and pledged to reinforce and enhance cyber defenses for networks and national infrastructures, and considered this step a high priority, in addition to the continues development of NATO's defensive capabilities as a part of its long term adaptation, since this enhances the cyber defense and collective flexibility of the alliance (21).

NATO has also established a number of institutions and teams responsible for the quick response to computer emergencies, these institutions and teams work around the clock and every day without stopping in order to provide technical and logistical support for NATO members in facing cyber-attacks, such as: Cyber Rapid Reaction Teams, NCI Agency in Belgium, and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia (22).

Sixth: Towards drafting a cooperative Arab strategy for regional cyber security:

The absence of a unified Arab vision and strategy that deals with cyber-attacks which Arab countries can work under is considered a threat to the stability of the region. As a result of the special nature of cyberspace including the difficulty of preventing cyber-attacks altogether in the first place because of zero-day attacks and bugs that are recently discovered, or the viruses and cyber weapons that are developed, not to mention the difficulty of tracing the attack source or the person responsible for it technically, all these reasons contribute to the complexity of the complete achievement of national cyber security.

Moreover, "deterrence" in its conventional method may not be achievable in the best scenarios in cyberspace, as it has not yet proven any actual success as it is the case of conventional deterrence. This itself presents a threat that escalates the seriousness of cyber conflicts that might reach a level of cyberwar. Therefore, it was necessary to draft a cooperative strategy that contributes to the development of cyber capabilities to defend Arab countries.

This could be achieved through the strategic cooperation between countries of the region regarding sharing the necessary information and data for digital evidence analysis, which assists in discovering cyber-attacks as they occur, work to mitigate its risks, tracking pirated financial transactions and encrypted transactions that might be used to finance rebel and terrorist movements. In addition to establishing a simulation of cyberwar between countries of the region to ensure the readiness of all cyber units in battle and providing technical and technological cooperation to develop cooperative cyber-attacking capabilities, to ensure the professionalism of the skill and intellectual level of the human cadre.

Conclusion:

The evolution of the form of war throughout history starting from using rocks, spears, spikes, swords, guns, rifles, to missiles, tanks, planes, submarines, and finally nuclear and hydrogen bombs indicate that whoever is not completely aware of the changing nature, age, and weapon of the next battle and strives to own it and develop it will end up defeated and following others among nations. As countries become more knowledgeable and advanced the more the destructive power of the weapons used become, hence, the weapon of the upcoming war will be stronger and more violent than any of the deadliest conventional bombs. As the soldiers fighting in this battle will be the robots and drones, and weapons will be codes, viruses, and programmed worms, the size of which will not exceed a few kilobytes but will have an impact that is more powerful than conventional weapons.

In this regard, we should be ready for the new phase of human war, which is certainly coming, it is cyberwar. This could be done by developing national cyber capabilities, establishing military cyber units inside the lines of the armed forces, developing an

arsenal of cyber weapons, and drafting a national strategy that operates under the framework of another national strategy that ensures the maintenance of the regional and national security.

Reference list:

1- Lewis, J. A (2006), Cybersecurity and Critical Infrastructure Protection, Center for Strategic and International Studies, . Washington, DC, 2006. on http://csis.org/publication/cybersecurity-and-criticalinfrastructure-protection

2- Committee on National Security Systems (2015), CNSSI No. 4009, P40, on https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

3 - Canongia, C., & Mandarino (2014), Cybersecurity: The New Challenge of the Information Society, Hershey, p 60.

4 - Cybersecurity Guide for Developing Countries (2009), ITU, on https://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf

5 - Dan Craigen, Nadia Diakun-Thibault, and Randy Purse (October 2014), Defining Cybersecurity, Technology Innovation Management Review, p15, on https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

6 -, Canada's Cyber Security Strategy (2010), Government of Canada, Ottawa 2010, Accessed OCT 3, 2021 on https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx

7- A Glossary of Common Cybersecurity Terminology (2021), National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security, DHS, on http://niccs.us-cert.gov/glossary#letter_c

8 - القرصنة الإلكترونية: بايدن يتعهد بعمل أمريكي ضد الهجمات الروسية (2021). BBC، متاح عبر الرابط https://www.bbc.com/arabic/world-57786593

9- Cybersecurity researchers warn of espionage campaign; India among the most affected nations, (2020), the hindu business line, on https://www.thehindubusinessline.com/info-tech/cybersecurity-researchers-warn-of-espionage-campaign-india-among-the-most-affected-nations/article32478808.ece

10- Newman, Neil, (2021), Russian hackers hit US and Europe. Is Asia the next target of a Massive Attack?, scmp, on https://www.scmp.com/week-asia/opinion/article/3140394/russian-hackers-hit-us-and-europe-asia-next-target-massive-attack

11- Jibilian, Isabella and Canales, Katie, (2021), The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal, businessinsider, on https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

12 - Global Cybersecurity Index 2020, (2020). P 25, ITU,

13- ميكا لوديرميلك، (٢٠١٩)، الأزمة الإيرانية تنتقل إلى الفضاء السيبراني، معهد واشنطن، للمطالعة: https://www.washingtoninstitute.org/ar/policy-analysis/alazmt-alayranyt-tntql-aly-alfda-alsybrany

14- Eastwood, Gary, (2017). How smart cities can protect against IoT security threats, Network world, on https://www.networkworld.com/article/3231988/internet-of-things/how-smart-cities-can-protect-against-iot-security-threats.html

15- The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology,(2014), Wired, https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/

16- إيهاب خليفة (2021). الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، دار العربي للنشر والتوزيع، القاهرة.

17- Trujillo, Clorinda, (2014). The Limits of Cyberspace Deterrence, P 45, the Air War College, Air University.

18- Metzger, Tobias, (2015), Deterrence theory in the cyber-century, Research Division EU/Europe.

19- إيهاب خليفة (2021). مرجع سبق ذكره.

20- Cyber defence, (2019), NATO, available on https://www.nato.int/cps/en/natohq/topics_78170.htm?

21- Warsaw Summit Communiqué, (2016), NATO, available on https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber

22 - Cyber defence, (2019) NATO, available on https://www.nato.int/cps/en/natohq/topics_78170.htm?

Received 06 Sep. 2021; Accepted 03 Oct. 2021; Available Online 31 Dec. 2021.

Keywords: Security studies, Fifth Domain, Cyberspace, National security, Cyber security.

الكلمات المفتاحية: دراسات أمنية، الميدان الخامس، الفضاء السيبراني، الأمن الوطني، الأمن السيبراني.

Production and hosting by NAUSS

* Corresponding Author: Ehab Khalifa
Email: ehabakhalifa@gmail.com
doi: 10.26735/ACPS7277