Legal Aspects of Cybersecurity

Menad icherak [*]
Faculty of Law and Political Science, Medea, Algeria
menad.icherak@univ.medea.dz

Belacel Yasmine Bint Nabi
Faculty of Law and Political Science, Medea, Algeria
belacel .yasmine@univ.medea.dz

Lamri Hakim
Faculty of Law and Political Science, Medea, Algeria
hakimlamri43@gmail.com

✱✱✱✱✱✱✱

Abstract:
  Cybersecurity is a crucial concern in today's digital age due to the increasing frequency of cyber-attacks and our growing dependence on technology. It is essential for individuals, companies, and nations to protect themselves from these threats.
 Hacking and cyber-attacks can be used by aggressive states to access sensitive information and disrupt critical infrastructure, resulting in significant financial and political consequences.
key words: Cybersecurity , cyber-attacks, political consequences, Hacking.

Introduction:
  In today's digital age, cybersecurity has become an increasingly important issue due to the emergence of cyber-attacks and the growing

---

[*]menad icherak

reliance on technology. It is imperative for individuals, businesses, and countries to protect themselves from these threats.

Cybersecurity threats come in various forms, including cybercrime and cyberattacks.

Digital threats can take many forms, including phishing scams, malware and ransomware attacks, and sophisticated hacking attempts targeting critical infrastructure and government systems.

 The impact of such attacks can be significant, resulting in data breaches, financial loss, and even physical harm. Therefore, it is essential to prioritize cybersecurity measures to mitigate the risk of these threats.

The significance of cybersecurity extends beyond individual companies and organizations, as it also has a substantial impact on national security and international relations.

Cybersecurity has become an essential component of modern warfare and interstate attacks. Hostile states can use hacking and cyber-attacks to gain access to sensitive information and disrupt critical infrastructure, resulting in significant economic and political consequences.

Therefore, it is essential to maintain strong cybersecurity measures to protect the confidentiality and integrity of a country's information and networks.

Based on these premises, we ask the following questions What is the relationship between cybersecurity and national security?

To answer this question, we have adopted the Descriptive Reporting Method and the following plan:

1. The idea of cybersecurity

Cybersecurity is a collection of lawful and also regulative structures, operations treatments along with technological as well as technical implies that stand for joint initiatives in between the general public and also economic sectors, in your area plus worldwide targeted at securing electronic room with an emphasis on making certain the accessibility of details systems strengthening electronic personal privacy, securing the discretion of info, together with taking all procedures to secure people.

Legal Aspects of Cybersecurity

1.1.   Definition of cybersecurity

Cybersecurity is composed of 2 words: protection as well as cyber as protection is the reverse of anxiety, i.e. safety and security. Safety is the resource of the verb aman, aman as well as amanah: The Penguin Dictionary of International Relations specifies it as a term that describes the lack of something that endangers uncommon worths.

When it comes to cyber: the term cyber is presently among one of the most usual terms in the global protection language as well as words suggests that it is a word of Greek beginning stemmed from a word suggesting the individual that guides the vessel where it is utilized allegorically for the controller and also it needs to be kept in mind that lots of chroniclers connect its beginning to the American mathematician Norbert Wiener 1948 He is the owner of cybernetics with his well-known publication "" Cybernetics or Control and also Communication in the Animal as well as the Machine"": Cybernetics or Control as well as Communication in the Animal along with the Machine. In his publication he described cybernetics as well as control as well as interaction in the pet and also the maker as well as male plus the maker to change the term maker with computer system after the Second World War (قره, 2019)

Cybersecurity or IT safety and security is a collection of procedures as well as treatments created to protect as well as safeguard networks, computer systems, software program as well as information from strike, damages, burglary plus unauthorized gain access to, in addition to from disruption or blockage of the solutions they supply. In this context in regard to computer system systems, the principle of safety and security is stood for by both cyber protection plus physical protection. (الأمير, 2018)

Cyber protection is the collection of technological, organisational along with management suggests made use of to avoid the unapproved usage, abuse together with recuperation of digital information and also interaction systems as well as the info they consist of with the objective of making certain the accessibility along with connection of info systems improving the defense, privacy plus personal privacy of

individual information as well as taking all needed actions to shield people coupled with customers from threats in electronic area. (شكري, 2019)

1.2.   Characteristics of Cybersecurity

Cybersecurity has a variety of attributes that identify it from various other areas one of the most crucial of which are:

1.2.1. Trust and also uncertainty:

The firewall software of the cybersecurity system has a sort of digital filter for the kind as well as nature of programs as well as modern technologies that are enabled to be triggered to make sure that it enables the flow of programs that currently have the count on of the customer and also the on-line store as well as have actually been validated as secure to make use of, and also stops harmful programs from getting in or making use of technicalities.

1.2.2. Protection from interior hazards:

 One of one of the most essential features of cybersecurity is the defense of the gadget versus inner hazards, which can be based upon the individual's absence of society or lack of knowledge in the area of info protection in which he might permit programs of unidentified beginning to be triggered or make use of devices that impact his individual safety and security or the level of sensitivity of sharing his info or among the devices he makes use of includes a destructive infection that his system must not have, cybersecurity rapidly notifies the specific or company to the threat it deals with as well as avoids this activity asap.

1.2.3. Protection from outside dangers:

Protection versus exterior dangers is one of the most crucial function of cybersecurity in which a firewall software is developed that has the ability to filter the outside threats that arise from managing the electronic globe beginning with the threats of risk-free e-mails, harmful web links, infections, or resolving system weak points or spaces that can be manipulated by a 3rd party in control as well as control.

1.2.4. Comprehensive presence:

Cybersecurity devices offer their individuals - people or firms - with an extensive sight of the staminas plus weak points of their systems to make sure that they can recognize technical spaces as well as job to fix them as promptly as feasible, while recommending the most effective method to stop their reappearance.

1.2.5. Continuous tracking:

Cybersecurity is based upon continual tracking, due to the fact that the firewall program does not function as soon as or at particular times, yet the system functions regularly with the goal of finding any kind of issue as quickly as it takes place as well as functioning to remove it rapidly stop it from triggering any type of damages plus keeping the safety of info as well as the safety and security of individuals for as lengthy as feasible.

1.2.6. Compliance with plans as well as legislations:

The key goal of Cybersecurity is to keep the discretion together with personal privacy of information along with details along with fighting damaging infections of all kinds as well as in order to attain this goal successfully the powers approved to its experts ought to not be made use of to go against the policy for which it was developed.

1.2.7. **Diversity**:

The cybersecurity system have to have integrated options for taking care of cyber dangers so that the system is not triggered to safeguard versus one sort of danger plus make it possible for one more however it has to evaluate, spot take care of as well as protect against all kinds of strikes that position a risk to the safety and security of details.

.1.3 Cybersecurity Objectives:

Cybersecurity is defined by a number of purposes, specifically (السمحان, 2020, p. 12)

-Improving the defense of functional modern technology systems in any way degrees and also their equipment coupled with software program elements, solutions plus information.

-Countering info safety strikes along with events targeting federal government firms coupled with public as well as economic sector organisations.

-Persistence of vital framework versus cyber-attacks.

-- Eliminating susceptabilities in computer coupled with mobile phones of all kinds.

-- Filling spaces in infotech systems.

-Withstanding malware made to create significant damage to individuals.

-Decreasing reconnaissance along with cyber reconnaissance at federal government plus specific degrees.

- Taking all required procedures to secure people together with customers from possible dangers in various locations of Internet usage.

- Educate people on brand-new devices and also treatments to deal with the obstacles of hacking their technological tools with the objective of harming, corrupting or taking their individual info.

1.4. Cyber dangers plus cyber assaults

Technical growths such as the expansion of the Internet plus mobile phones and also the schedule and also small cost of broadband Internet accessibility by means of cell phones have actually brought about a rise in the variety of Internet individuals as well as a raised dependence on these modern technologies for financial along with social growth. Nevertheless the visibility that identifies the Internet together with area as a whole has actually made it vulnerable to infractions and also criminal tasks and also individuals of area have actually come to be susceptible to different cyber risks together with strikes by cyberpunks.

1.4.1 Cyberspace:

The room or material as well as the planetary option that permits individuals to take part in it and also William Gibson explains it as the electronic globe, which is a local area network as well as digital interactions and also is a fictional local area network that includes a large quantity of info that can be acquired to accomplish wide range as well as power, where the connection in between the physical globe and also the real life is obtaining better to make sure that computer

system individuals obtain nonexistent experiences that they obtain with this usage and also electronic parts impact the real life, plus the power of the computer system has actually raised, which has actually made individuals see area as a parallel globe to the fact we reside in and also the digital room (العباسي, 2016)

1.4.2. Cyberterrorism:

Dorothy Denning specifies cyberterrorism as an expression of the merging of terrorism plus the computer system globe, as well as is the prohibited use pressure together with risks to strike computer systems, networks and also the info kept in them in order to frighten as well as coax federal governments and also their individuals to accomplish political along with social objectives, as well as for it to be thought about terrorism it has to cause scare tactics as well as browbeating of federal governments, individuals and also residential or commercial property or a minimum of reason damages as well as worry, in addition to casualties, physical injury, surges, major financial damages strikes on framework, together with interference of important solutions. (وآخرون, 2020)

There is no agreement on the interpretation of cyberterrorism yet it is usually described as a brand-new kind of terrorism that drops within the structure of cybercrime and also acquires its name from using info and also interaction innovation devices alongside sources to execute terrorist acts that go beyond regional as well as nationwide measurements plus have a considerable effect on global safety (حكيم, 2018, p. 106)

1.4.3. Cyberwarfare:

It is the collection of digital treatments including making use of some pleasant digital systems plus indicates to discover the electro-magnetic radiation emerging from the adversary's systems indicates plus numerous digital devices, with the purposeful use electro-magnetic power to impact these systems together with ways; to stop, reject or minimize the opponent's exploitation of the electro-magnetic area in addition to to secure the electro-magnetic waves appearing from

pleasant digital systems as well as implies from being checked out or affected by the adversary. (الصحراء)

1.4.4. Cyber **reconnaissance**:

 It has actually spread out in the brand-new centuries with the expansion of hacking techniques. Occasionally the hacking is done by insignificant individuals simply to swipe essential details, like what occurred to the United States Pentagon in the last 2 years by individuals that are not connected to Al-Qaeda, however instead minor individuals, as well as the French Ministry of Defence site was hacked 2 years ago to swipe details on reconnaissance, manoeuvres and also the French projectile system coupled with not just the hacking is not restricted to the Almighty.

2. Cyber warfare and its impact on the protection of statesThe technological advancement of the electronic globe is a transformation in all areas, particularly in the area of info which has actually been made use of in every feasible method with the goal of straight as well as in a roundabout way affecting individuals that travel through this area coupled with manipulating the mental facet of them particularly in times of situation, which is a productive ground for highlighting its several plus various techniques of publicity, spreading out reports media false information, copyright adjustment, mind control the individual, resetting him plus attempting to adjust him to certain goals of whoever is exploiting him.

2.1. Dispute change in cyber war

As the online world has actually helped to enhance communications in between people throughout nations, promoted the exchange of details as well as information as well as advertised the architectural modification of the decision-making procedure within the state, from dependence on main organizations to the communication of main coupled with informal entities, teams as well as people within the state via social media networks, modern technology has actually transformed the kinds of human battles along with disputes throughout the ages from conventional battles making use of swords as well as lances to a brand-new kind of battle, specifically cyber battles utilizing a various sort of tools stood for by trojans that have the capacity to create damage equivalent to that of tools of mass damage.

2.1.1 Major changes worldwide's non-traditional terrible disputes

According to Carl von Clauswetter, battle is absolutely nothing greater than a way to accomplish a details end which is to require the adversary to send to the will of the state and also to apply tranquility on terms that fit the passions of the victorious event. (Jan Angstrom, 2004, p. 4)

The key purpose of battle generally is to accomplish the nationwide passions of the state, i.e. to keep survival plus safety and security to sustain security along with to boost the impact, power as well as local standing of the state hence surpassing the function of battle which is simply to accomplish success on the field of battle by beating the assailant state, regulating the objected to region, toppling the routine as well as compeling the challengers to transform their practices.

Nonetheless, offered the existing conditions in the worldwide sector plus the growths related to the numerous significant together with educational growths together with their repercussions a number of significant changes have actually taken place in the conventional ideas of battle as well as different disputes.

We summarise them as follows (الوهاب, 2017, p. 6)

-The decrease in interstate disputes, instead of the rise in interior disputes: These are problems in between the state plus equipped non-state stars without rejecting that some states get involved in these interior disputes to sustain their allies.

Boosted participation in between equipped non-state stars and also transnational well organized criminal activity teams: regardless of their entirely various goals, usual passions lead them to work together, causing enhanced safety and security mayhem as well as the presence of regions outside the control of state organizations.

-The expansion of protracted disputes: The events to the problem recognize that they can not accomplish their objectives or solve the problem in the short-term, so they take on the technique of "" minimal interaction"", i.e. preventing straight army participation in disputes and also relying upon proxies of signed up non-state stars.

Control of technical advancement by equipped non-state stars: In specific dual-use products and also modern technologies that are

traded for business objectives as well as can be repurposed for terrorist or battle procedures such as filling drones with nitroglycerins or utilizing 3D printers to produce tools and also nitroglycerins.

-The obscuring of the lines in between battle and also tranquility: Especially as states coupled with armed stars consider info war versus their challengers.

The decrease of commitment to the nation-state in the centers of armed dispute: This is because of the increase of second loyalties to entities or triggers that go beyond state boundaries such as the mission to develop a caliphate or commitment to non-state entities such as a certain ethnic culture or religion which has actually caused the spread of spiritual, patriot coupled with sectarian extremism.

2.2. Asymmetric risks: New problems for nationwide safety as well as

Generally, we can not discuss the nature of uneven or unbalanced dangers plus recognize their numerous measurements without acknowledging as well as recognizing the preliminary significances plus undertones increased by the principle of danger as a sensation or problem that interrupts safety coupled with security.

Danger is etymologically specified from the verb endanger which is the outcome of causing damage along with damages, i.e. danger relates to anything that would certainly obstruct the procedure of structure safety and security or bring about a reduction in its feeling. (صباح, 2019)

The etymological significance of hazard in the English language is Threat, while in the French language it describes the significance of Menace, as well as in the Latin language Trudere is identified with the significance of press and also according to Webster's Dictionary a danger is A declaration or expression of purpose to hurt, ruin or penalize by vengeance or scare tactics and also the significance of the term danger in the French language, according to Le Petit Robert thesaurus, refers to: The means in which horror is repainted on somebody's face, with the intent of making them fear the injury one means to bring upon on them. (موقع العلاقات الدولية, 2019)

In calculated terms, danger takes place when the dispute of nationwide passions as well as goals gets to a phase where it is difficult to

discover a relaxed option that supplies the state with a minimum of its political, financial, social and also army protection for its poor capacity to stabilize exterior stress which might compel the contrasting events to consider using armed forces pressure revealing various other events to the danger. (حربي، 2008, p. 28)

Safety dangers are specified by Richard Ullman: An across the country protection danger is an act/action or collection of occasions that, over a reasonably brief time period considerably minimizes the lifestyle of a state's residents or considerably decreases the variety of plan choices readily available to a state's federal government, exclusive entities as well as non-governmental organisations (people, teams as well as companies) within the state. (صباح, 2019)

Cyber dangers describe those assaults that make use of digital devices as well as networks such as the Internet as well as computer systems to harm various other digital gadgets or networks or to swipe the details on them. The electronic devices of the danger refer to both the device of the assault, i.e. the systems utilized to release it, as well as the electronic devices of the target subjected to it. Digital targets might be subjected to non-electronic strikes, such as kinetic and also physical strikes, or electro-magnetic activities which trigger damages as well as potentially disable them (شفيق, 2020)This sort of hazard is specified by an inequality of power in between its stars where the weak event looks for to manipulate the susceptabilities of the more powerful celebration.

This pattern of danger has actually ended up being progressively common recently (سليم, 2019, p. 1131)

Contemporary disputes are no more restricted to standard war with clear limits as well as measurements. Rather, they have actually developed right into an intricate battleground where all offered ways both standard as well as non-conventional, strait as well as invalid, are used. This is especially noticeable in light of technical improvements as well as the info as well as interaction transformation, which have actually modified much of the dominating ideas of problem (such as battle, problem, and also disagreement). The main goal of these

disputes is to undermine the opponent from within, as it is taken into consideration one of the most efficient approach for accomplishing success.

The development of problem has actually gathered substantial academic passion from armed forces experts and also planners looking for to realize, keep an eye on and also track these improvements in war,This has actually brought about the growth of brand-new ideas associated with the transforming patterns of battle plus their future expectation. (عربية, 2022, p. 466)

 The ideas that are taken into consideration essential consist of fourth-generation battles, fifth-generation battles, crossbreed battles, grey areas, unlimited battles, 21st century battles, as well as various other brand-new terms in this regard. The change to a pattern of details battles motivated previous United States Secretary of Defence William Perry to advise regarding its risk plus the hazards it poses, mentioning: We are presently residing in a period where details is the driving pressure, coupled with technical improvements have actually transformed war and also its prep work. (Roger C. Molander, 1996)

In the exact same context, the 2010 United States knowledge file highlighted the value of buying net as well as social networking websites.

The knowledge area has an essential duty in improving web protection by identifying rivals' tasks and also susceptabilities in addition to their purposes. It is likewise crucial to mobilise even more sources to find as well as take down net hazards as well as broaden social media networks.

Appropriate experience need to be shown to the knowledge area, allied knowledge companies as well as the technical scholastic neighborhood.

In addition, significant changes in the nature of electronic disputes need to be thought about.

2.3   Major shifts in the nature of cyber conflict

In the last few years there has actually been a considerable growth in infotech that has actually affected all areas, consisting of global connections. This has actually transformed electronic right into a

brand-new sector for numerous global disputes, which is used for both private citizen and also army functions.

Electronic battlegrounds have actually come to be an area for problems in between different stars, consisting of both state plus non-state entities. Cyber war varies from typical battles in regards to the nature of tasks, stars entailed coupled with ramifications for global safety style. It likewise offers brand-new chances to reply to arising hazards. (الصادق, 2018)

2.3.1 Adjustment in Global Security Threats

The partnership in between electronic as well as worldwide protection has actually come to be significantly vital as a result of the extensive fostering of e-government by several nations as well as the expanding variety of individuals of interaction together with infotech worldwide. This has actually resulted in nationwide data sources being susceptible to exterior direct exposure making them at risk to cyber strikes, publicity, false information, reports, provocations, together with assistance for inner resistance to the judgment program with electronic. It is critical to resolve these concerns to make certain the safety and security of nationwide data sources as well as protect against possible hazards. (الحسين, 2021, p. 168)

Vital facilities connected to nationwide rate of interests such as power, interactions, transport, federal government solutions, ecommerce, financial, as well as banks, go through cyber assaults. The National Information Infrastructure has actually made these passions adjoined as well as international protection currently depends on the worldwide neighborhood's capability to stop aggressive acts in electronic (الصادق, 2018)

These symptoms have actually pertained to highlight the non-peaceful uses electronic as well as the danger to worldwide cybersecurity positioned by all stars in the worldwide info culture. Any kind of entity linked to the ICT network can be influenced by various other entities attached to the network or by the nature of the hazards to the network as well as its procedure. This has financial plus safety and security ramifications plus can impact political and also social

security. It is commonly thought that depend on plus safety and security are 2 crucial columns of the worldwide info culture.

The arrangement of technical together with legal assistance along with the production of a good atmosphere for the growth as well as security of the technical industry have actually ended up being critical columns of this area. (الصادق, 2018)

The globe is encountering brand-new components of worldwide safety and security because of numerous variables. Among one of the most considerable elements is the boosting link of the international details facilities to electronic which makes it susceptible to cyber assaults. This susceptability is more exacerbated by the growth of non-state stars' use electronic.

The calculated benefits of cyber strikes have actually resulted in the opportunity of army work as a result of the dependancy of states on digital systems in their important centers. Digital can be made use of to make the most of the power of states by developing a benefit, prevalence or impact in various settings. Hence, states have actually established an electronic technique that includes incorporating along with working with abilities to run in electronic with various other functional locations to attain nationwide objectives. (الصادق, 2018)

2.3.2.   Altering Principles of Safety as well as Problem in Cyberspace

Cyber room has actually altered the nature and also features of protection power as well as problem in the worldwide field whether at the academic or used degree plus has actually come to be a clear impact as well as proof in worldwide connections: (الصادق, 2018)

- Cyber safety is no more restricted to the technological measurement yet has actually increased to various other measurements in light of the decrease of state sovereignty coupled with the expanding connection in between safety as well as modern technology as a whole particularly with the opportunity of subjecting the tactical rate of interests of states to risks plus hazards as well as these advancements have actually compelled a reconsidering of the principle of nationwide safety and security, which suggests securing the essential worths of culture as well as maintaining resources of risk far from them, coupled

with the lack of anxiety that these worths might be struck. On the various other hand the improvement of cyber room right into a worldwide sector that goes beyond state boundaries has actually developed a natural web link in between a state's inner cyber safety as well as the safety of cyber room which develops the basis of worldwide cumulative safety and security, specifically when faced with threats that intimidate all stars in the worldwide info culture.

-Cyberspace plus.sourceforge.net/ has actually played a vital function in the prise of power or the procurement of its standard aspects in worldwide loved ones, as supremacy in this area has actually come to be a crucial aspect in the conduct of efficient procedures ashore, sea, air plus room, and also the reliance of battle ability in cyberspace on technical command as well as control systems.

Cyber power has actually added to the strengthening of state soft power, as cyberspace has actually ended up being a theatre for seditious assaults pertaining to the circulation of disinformation, emotional combat, affecting popular opinion patterns, plus hidden and also reconnaissance tasks. On the various other hand, the development of this pattern has actually added to nations enhancing their costs on cyber support plans, securing their nationwide networks from the danger of risks as well as constructing nationwide establishments for cyber defense(الحسين, 2021, p. 169)

The connection of cyber room to the development of brand-new patterns of dispute: as a location of problem in between various stars and also an expression of the problem of passions as well as worths whether in between state or non-state stars, plus since cyber room is transnational and also conveniently obtainable, the circle of cyber problem has actually increased, the variety of assailants has actually enhanced along with disputes have actually arised over the purchase of security plus protection devices, the advancement of cyber offending capabilities and also the race to get power as well as supremacy together with increase the capacity to raise impact coupled with effect at the regional together with worldwide degrees. This cyber problem might be political in nature a problem over the

development of info, the burglary of commercial keys, or a problem over clinical development or control of worldwide markets.

The connection in between cyber room as well as worldwide safety has actually arised specifically with the development of the fostering of e-government by several nations along with the development of the variety of individuals of interaction and also details innovation on the planet where nationwide data sources remain in a state of exterior direct exposure subjecting them to the danger of cyber strikes along with publicity as well as false information, spreading out reports requiring inflammatory activities, sustaining inner resistance to the ruling regimen plus offering product together with ethical assistance via cyber room. (الصادق, 2018)

The cyber domain name in the Arab area as an example has actually played a vital function in causing a collection of adjustments of a political and also safety and security nature specifically after 2011 which have actually had a huge effect on culture plus its connection with the state, also straight impacting the "" Arab state"" with its failing and also the collapse of state organizations specifically in those nations that experienced a decrease in modernity as well as growth as when it comes to Yemen as well as Libya, while it tackled a political duty in various other nations, as when it comes to Egypt together with Tunisia, which are identified by the advancement of the structures of the state along with the civil nature of their individuals, along with making use of the "" cyber domain name"" incorporated the political as well as armed forces duty when it come to Syria. (الحسين, 2021, p. 174)

The Arab area has actually been revealed via the cyber domain to mental combat focused on affecting the important mass of young people via socials media whether by intrigues based upon political, spiritual or factional distinctions as well as on the various other hand, outside powers have actually practiced cyber treatment to impact safety as well as security whether by fuelling factional disputes, such as Iran's function in feeding social media sites accounts to sustain as well as politically prompt Shiites in the Gulf nations or by utilizing the cyber domain name to improve monitoring coupled with reconnaissance on the nations of the area by local powers such as

Israel, Iran along with Turkey or with reconnaissance by various other worldwide powers.

Conclusion:

In conclusion, cybersecurity is a vital aspect of our digital lives, protecting sensitive information and safeguarding against potential digital threats. The importance of cybersecurity is reflected in its impact on individuals, businesses, and even national security. It is essential to prioritise cybersecurity measures to mitigate the risk of cybercrime and cyberattacks and ensure optimal protection of information and networks.

Cyber security threats have increased as the digital environment has become an area of transformation in the concepts of conflict, warfare and power. The misuse of digital technology has led to a significant increase in security threats in the cyber world.

 The digital environment is now seen as one of the greatest threats to states, posing a threat to national security and national sovereignty.

This growing threat to national security, critical infrastructure and privacy is referred to as cyber warfare.

 Cyber-attacks are one of the most common cybersecurity threats faced by States and can pose a threat to the security of States and their various entities.

Among our searchings for:

One of the characteristics of cyber warfare is the inability to distinguish between civilian and military targets in cyber warfare attacks and the near impossibility of imposing international protection. In the light of what has been discussed, we have decided to make some recommendations, the most important of which are:

-Adopting measures that make security an absolute necessity, especially with regard to the software and hardware used in communication technologies.

- Establishment of centres for information security and communication emergencies, which cooperate according to clear and transparent mechanisms.

-Qualifying special military security units to cooperate internationally with organisations working to combat, reduce and mitigate risks.
-Make cyber security part of development plans.

Bibliographie

Jan Angstrom, I. D. (2004). *Rethinking the Nature of War.* Routledge.

Roger C. Molander, A. R. (1996). *Strategic Information Warfare.* Consulté le 04 16, 2023, sur rand.org: https://www.rand.org/pubs/monograph_reports/MR661.html

الأمير, ح . ب. (2018). *تحديات الأمن السيبراني* Consulté le 01 21, 2023, sur مركز الدراسات الاستراتيجية CSS: https://kerbalacss.uokerbala.edu.iq/wp/

الحسين, ب. ع.-ب. (2021). *التهديدات الإلكترونية والأمن السيبراني في الوطن العربي.* مجلة نوميروس.

السمحان, م . ع. (2020). *متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعو.* مجلة كلية التربية، جامعة المنصورة.

الصادق, ع . ع. (2018, 03 11). *أنماط وتحديات جديدة للأمن العالمي-الهجمات السيبرانية.* المركز العربي لأبحاث الفضاء الإلكتروني ACCR: Consulté le 04 17, 2023, sur https://www.accronline.com/article_detail.aspx?id=29088

الصحراء, م . م. (s.d.). *الحرب الإلكترونية.* Consulté le 04 2023, 01, sur موسوعة مقاتل من الصحراء: http://www.muqatel.com/openshare/Behoth/Askria6/ElectroWar/sec03.doc_cvt.htm

العباسي, ر . ع. (2016). *أثر الإرهاب الالكتروني على تغير مفاهيم القوة في العلاقات الدولية 2001-2015- دراسة حالة تنظيم الدولة الإسلامية في العراق والشام (داعش).* ألمانيا: المركز الديمقراطي العربي.

الوهاب, ش . ع. (2017, 11). *التحولات الرئيسية في المواجهات العنيفة غير التقليدية -حروب الجيل الخامس.* في العالم سلسلة دراسات المستقبل، المستقبل للأبحاث و الدراسات المتقدمة.

حربي, س. ع. (2008). *دراسة نظرية في المفاهيم والأطر-مفهوم الأمن مستوياته وصيغه وأبعاده.* المجلة العربية للعلوم السياسية.

سليم, ب. (2019, 09 02). *العقيدة الأمنية الجزائرية وإشكالية التكيف مع التهديدات الجديدة.* مجلة العلوم القانونية والسياسية.

شفيق, ن. (29 01, 2020). *أشكال التهديدات الإلكترونية ومصادره*. Consulté le 04 17, 2023, sur المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات ECCI: https://www.europarabct.com/%D8%A3%D8%B4%D9%83%D8%A7%D9%84-%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%88%D9%85%D8%B5%D8%A7%D8%AF%D8%B1%D9%87/

شكري, ح . ع. (2019). *الفضاء الإلكتروني-المجال الخامس*. Consulté le 02 20, 2023, sur المعهد المصري للدراسات: eipss -eg-org.cdn.ampproject.org

صباح, ب. (08 09, 2019). *التهديدات الأمنية*. Consulté le 4 14, 2023, sur الموسوعة السياسية: https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D8%A7%D8%AA%20%D8%A7%D9%84%D8%A3%D9%85%D9%86%D9%8A%D8%A9

عربية, ب . ر. (12 06, 2022). *التهديدات اللاتماثلية في الفضاء السيبراني: نموذجا حروب الجيل الرابع*. *دفاتر البحوث العلمية*, pp. 456-477.

قره, ف. (28 08, 2019). *الأمن السيبراني*. Consulté le 01 20, 2023, sur الموسوعة السياسية: https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A#google_vignette

موقع العلاقات الدولية. (24 11, 2019). *تعريف التهديدات الأمنية والمصطلحات المشابهة*. Consulté le 04 13, 2023, sur www.elsiyasa-online.com

وآخرون, س . ر. (02 02, 2020). *سياسة مكافحة الإرهاب الإلكتروني...مصر والسعودية نموذجا*. Consulté le 02 15, 2023, sur المركز العربي للبحوث والدراسات: http://www.acrseg.org/41483