CYBER THREATS

AND THEIR IMPACT ON PROTECTING INFRASTRUCTURE AND VITAL SERVICES

ماعت للسلام والتنمية وحقوق الإنسان
Maat For Peace, Development, and Human Rights

Introduction

International interest in the relationship between security and technology has increased due to two significant dimensions. The first relates to technological progress, the rapid spread of communication and information technology globally, and using it in vital facilities through its multiple applications, whereas the second relates to the possibility of using that progress and the resulting new tools and mechanisms as a means and mediator to threaten the functioning of vital facilities and the global infrastructure due to its transgression of the sovereign borders of states. Actors of all kinds non-peaceful states to non-state actors, use it as a fertile environment. They use cyberspace as an arena for the cold war, psychological warfare, and a war of ideas. They use it to wage wars and terrorism between states, or they use individuals, terrorist groups, hackers, or organized crime in a way that affects cyberspace's civil or peaceful nature.

Cyberspace transformed into a new field for international interactions, so it becamed used in both civil and military. Cyber attacks appeared through two patterns, the first related to soft power in the conflict through cyberspace using wars of ideas and psychological operations. The other pattern is hard power, using viruses and cyberattacks as hostile activity. In this context, cyberspace has become a field for conflicts between all kinds of players, whether state or non-state. Cyber wars are different from traditional wars in the nature of activities, actors, and repercussions on the global security structure and in the opportunities to respond to these new threats. In addition, these attacks have become a critical threat to the work of civil society organizations and human rights defenders.

Thus, cybersecurity threats are subject to the rules and regulations of international law in light of recent technological developments and cybersecurity challenges. Cybersecurity is weapon countries seek to possess and protect from any breach to ensure military information. Also, despite the evolution of the means and methods of war, when drafting the Geneva Conventions in 1949, international humanitarian law was applicable and respected to all parties' activities during the armed conflict. However, it has to develop the law to ensure that it provides adequate protection to the civilian population cannot be ruled out as cyber technology evolves or as its humanitarian impact becomes better evident; States should decide this for themselves.

Hence, Maat for Peace, Development and Human Rights shows interest in the issue by presenting this research paper on the impact of cyber threats on the infrastructure and vital services of countries, through several axes:

First: What are cyber attacks and their types?

Studies and reports define an electronic or cyber attack as a malicious and deliberate attempt by a party, a country, an institution, a group of individuals, or an individual, to penetrate institutions that work on Internet systems. Electronic or cyber-attack aims to access data, and cause extensive material damage by closing, destroying, or disabling it. It also aims to affect the quality of the service it provides or extract data and information from it to steal it and manipulate data to undermine confidence in the work of these institutions[1].

The United Nations estimates indicate that some electronic attacks damaged parts of the service infrastructure of government institutions in some countries and affected electricity and water supplies, hospitals, and databases in financial institutions and government ministries[2]. When electronic hostilities increased on the information infrastructure of countries to achieve overlapping purposes (political, economic, criminal, etc.), the concept of electronic warfare changed. Some people prefer cyberwarfare to describe electronic hostile activities, including cyberattacks, cyberterrorism, and others. [3]

Electronic attacks have many types according to the method used in electronic penetration or the ultimate goal of the operation. Malware and viruses damage the Internet that operates various services; the Trojan horse program is one of the most prominent examples, which causes the Internet to be disrupted or controlled remotely. Some parties send e-mail messages to deceive the target party to steal information or control them. This technique is known as phishing and uses against human rights defenders and civil society activists. Some parties try to use brute force to try to stop or disable certain online services in what is known as a denial of service attack. Some parties try to use brute force to stop or disable certain online services in what is known as a denial of service attack. Man-in-the-middle attacks (MITM) are common cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The perpetrators of electronic attacks exploit the gaps in the Internet systems based on the management of some services to access them and control their data to control them and achieve their goals through attacks called injection attacks[4] .

[1] التعرف على الهجمات الالكترونية وكيفية الدفاع ضدها، الخدمات والاستشارات، https://ibm.co/2YUxKHM
[2] استخدام المرتزقة كوسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير المصير ، الأمم المتحدة الجمعية العامة ، يوليو 2020، https://bit.ly/3vgL8BJ
[3] - أنماط الحرب السيبرانية وتداعياتها على الامن العالمي، السياسة الدولية، الرابط، http://www.siyassa.org.eg/News/12072.aspx
[4] ما معنى الهجمات الالكترونية واشهر الهجمات السيبرانية، مؤسسة غانم لتقنية الحاسب الآلي ، https://bit.ly/3p7nvud

Second: Cyber attacks and international humanitarian law

Can the principles and rules of international humanitarian law be applied to states' use of cyberspace to launch cyberattacks during armed conflicts? Because when legal rules related to the means and methods of warfare were enacted, there were no cyberattacks. There were the Hague Conventions of 1899-1907, the four Geneva Conventions of 1949, and the two Additional Protocols of 1977, so no special provisions were enacted to regulate cyber attack use legally[5].

In light of the law of war provisions, new means and methods of fighting development were expected, such as article 36 of Additional Protocol I annexed to the Geneva Conventions. It stipulates that "any High Contracting Party shall, when studying, developing, acquiring a new weapon, instrument of war, or adopting a method of warfare, verify whether this is prohibited in all or some cases under this Annex Protocol." Or any other rule of international law to which that High Contracting Party is bound. Thus, this article lays down the general framework for organizing using new means and methods of fighting in armed conflicts[6]. The provisions of this article also indicate that, in light of the law of war, countries that acquire or develop modern weapons must follow a new method of fighting and determine the legality of their use. This text also implicitly states that all rules of the law of war apply to modern means and methods of warfare. In principle, in the absence of a specific text, the general text has to apply.

Also, based on the principles of international humanitarian law, the Martens Clause is an effective way to confront the technical developments that define the means and methods of combat. It was mentioned for the first time in the second Hague Convention of 1899; It stipulates: "In the case where a treaty or customary law does not apply, civilians and military personnel enjoy the protection of the principles of international law derived from established custom, from humanitarian principles, and the dictates of public conscience." By analogy with this, weapons repugnant to public conscience may be prohibited[7].

Electronic attacks, as one of the modern weapons in warfare, are subject to many governing principles of international humanitarian law, especially:

- According to the text of Article 48 of Additional Protocol I of 1977, the principle of distinction requires that parties to an armed conflict distinguish at all times between

[5] - حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني، 2020، الرابط، https://bit.ly/3bHUG2J

[6] - راجع المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جينيف 1977، الرابط،
https://www.icrc.org/ar/doc/resources/documents/misc/5ntccf.htm

[7] - صلاح جبير البصيصي، دور محكمة العدل الدولية في تطوير مبادئ القانون الدولي الإنساني، الرابط، https://bit.ly/3xXrYlQ

civilians and civilian objects on the one hand and combatants and military objectives on the other.

- Paragraph 2 of Article 51 of the same protocol stipulates that "the civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence aimed primarily at spreading terror among the civilian population are prohibited".
- Article 52 of the Protocol: "Civilian objects shall not be the object of attack or deterrence attacks." Article 55 of Protocol I also prohibits the use of means and methods of warfare that are intended or expected to cause severe, widespread, and long-term damage to the natural environment and thus harm the health or survival of populations and prohibits deterrence attacks against the natural environment. Article 56 also protects engineering works and installations that contain dangerous forces.
- The International Court of Justice confirmed in its advisory opinion in 1966 that international humanitarian law is based on two fundamental principles, the first of which states that states should not make civilians a target of attack. The second principle prohibits using weapons that would cause unjustified pain; this principle in the Hague Regulations Concerning the Laws and Customs of War on Land of 1907, "the right of the belligerents to choose the means and methods of warfare is not unlimited." Thus, given the obligation of these rules, we see that they apply to cyber attacks[8].

Third: The impact of the escalation of cyber attacks against the infrastructure of countries

Cyberspace and international security are linked because many countries depend on electronic governments, and the users of means of communication and information technology in the world are increasing. The national databases are exposed externally, so it is at risk of cyberspace attacks, propaganda, misleading information, spreading rumors, calling for provocative actions, supporting internal opposition to the ruling regimes, and providing material and moral support through cyberspace.

National interests that are linked to critical infrastructure became at risk of attack, energy, telecommunications, transportation, government services, e-commerce, banking, and financial institutions. Cyberspace made those interests linked to each other in one work environment. It is known as the national information infrastructure and its connection to the global information infrastructure. Global security has become related to the international community's ability to take measures to protect against exposure to hostilities and the misuse of cyberspace[9].

[8] - حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني، 2020، الرابط، https://bit.ly/3bHUG2J

[9] - الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، الموسوعة الجزائرية، الرابط، https://bit.ly/2J3GFua

Cyberattacks against the critical infrastructure of countries have increased dramatically in recent years, and this has affected some economic and civil rights. Infrastructure is considered the key to developing services in societies, and thus hindering it from its work means a threat to the rights related to the lives of citizens. New determinants of global security have also emerged due to the increasing interdependence of the global information infrastructure with cyberspace, which makes it vulnerable to electronic attacks, especially with the expansion of the movement of non-state actors in its use.

For example, those attacks undermined the right to access medical and health care, the right to access clean water and sanitation services, access to electricity, the right to development, and the political and civil rights associated with access to information. Recently, hospitals and medical care facilities have become the most targeted places for cyber-attacks. Attackers use ransomware to target hospitals and healthcare institutions across Europe and the United States of America because they depend on the Internet for all of their business. It is estimated that cyber attacks on hospitals increased during the spread of the COVID-19 pandemic[10].

In September 2020, the first human death was due to a ransomware attack. The attack caused a breakdown in information technology systems at the German Dusseldorf University Hospital. A woman died after they moved her to another city 20 miles away for treatment, and the hospital could not receive any emergencies. It was reported that the attack did not target the hospital itself but rather the Heinrich Heine University, which was addressed to pay the ransom[11]. In May 2017, a cyberattack hit the National Health Service in England, preventing staff from using their computers and forcing some hospitals to transfer patients to other hospitals[12].

With the spread of the Covid 19 pandemic, the targeting of health systems increased worldwide. In October 2020, the FBI warned of an imminent wave of cyberattacks on hospitals amid the Corona pandemic, with an indirect reference to the possibility of the Russian government being involved in the matter.[13] Some cyberattacks also reached Irish Health Service Systems, targeting the Irish Health Services Authority and encrypting patient data in May 2021. In this regard, the attack affected some hospitals, which led to the cancellation of consulting services for cancer patients, and the disruption of radiology and diagnostic systems,

[10] Microsoft. Cyberattacks targeting health care must stop . November 2020 . https://bit.ly/3vf3brW

[11] - الامن السيبراني في 2020 بين الفرص والتحديات والحماية، الموسوعة الجزائرية ، 2021، الرابط، https://bit.ly/3yGFWu8

[12] Massive ransomware cyber-attack hits nearly 100 countries around the world ،theguardian،https://bit.ly/3vf4sil

[13] الـFBI تحذر من موجة وشيكة من الهجمات الإلكترونية على المستشفيات، روسيا اليوم ، أكتوبر 2020 ، https://bit.ly/3mSBVLS

the perpetrators of the attack call themselves Conte Locker[14]. In June 2021, ransomware targeted the IT network of the health system in Georgia, which forced them to shut down the IT systems to reduce the potential effects of the attack, so that the health system switchs to backup operating methods, including paper documentation for at least a week since the attack was launched[15].

On the other hand, the attacks on water and electricity stations led to the disruption of services, not to mention the poisoning of water at times. For example, in January 2021, a cyberattack attempted to poison a water treatment plant serving parts of the San Francisco Bay Area in the United States of America[16], while in November 2017, the situation of the power grid in the United States became increasingly worrisome after several power plants were hacked, which contributed to the power outages in factories, workplaces, and homes. In the same context, there was a complete power outage in Ukraine between 2015 and 2016. In one of the attacks, it was estimated that the Russian (Sandworm Team) had penetrated power stations in Ukraine after the conflict on the Crimean front, which contributed in power outage throughout the country, and about a quarter of a million Ukrainian citizens were affected[17]. In the same context, on May 7, 2021, the United States was subjected to an attack targeting one of the largest gasoline and diesel pipelines that supply the eastern coast with fuel through a 5,500-mile network, which resulted in its closure and cessation of work, and this negatively affected the lives of citizens on the coast[18]. In July 2021, 200 American companies were affected by electronic hack operations; this affected the provision of services to citizens[19].

- **Cyber threats in the Arab region**

The Arab region has also been subjected, through the cyber domain, to psychological warfare, where external forces have practiced cyber-interference to influence security and stability, whether by fueling sectarian conflicts, such as the role played by Iran in fueling accounts on social networks to support Shiites in the role of the Gulf and incite them politically or by employing in the cyber field to enhance surveillance and espionage on the countries of the region by regional powers such as Israel, Iran and Turkey, or through espionage from other international powers[20]. Some industrial sectors and government agencies in the region were subjected to electronic attack, which affected the level of public service provided to citizens

[14] قراصنة يهاجمون هيئة الخدمات الصحية الأيرلندية ويطلبون 20 مليون دولار فدية، الشرق ، مايو 2021 ، https://bit.ly/2YPQY0G
[15] مخاطر متزايدة دلالات تصاعد هجمات الفدية عالمياً، مركز المستقبل للأبحاث والدراسات، يوليو 2021 ، https://bit.ly/3DJzYIE
[16] مركز استخباراتي: قرصان يحاول تسميم مياه الشرب إلكترونيا في أمريكا، الوطن ، يونيو 2021 ، https://bit.ly/3lM6jIL
[17] القرصنة الإلكترونية تهدد شبكات الكهرباء العالمية، الروية، نوفمبر 2017 ، https://bit.ly/3BRo9PW
[18] مخاطر متزايدة دلالات تصاعد هجمات الفدية عالمياً مرجع سابق ذكره
[19] تقرير هجوم إلكتروني روسي يخترق أكثر من 200 شركة أمريكية، الدستور ، يوليو 2021 ، https://bit.ly/3DM0ilj
[20] - الامن السيبراني في 2020 بين الفرص والتحديات والحماية، الموسوعة الجزائرية ، 2021، الرابط، https://bit.ly/3yGFWu8

or undermined public confidence in government institutions. For example, Saudi Aramco was subjected to increasing electronic attacks through malicious software, which harms the economy of the Kingdom of Saudi Arabia and is reflected negatively on the economic rights of Saudi citizens[21].

The cyber domain also affected the inter-Arab relations between the Arab countries, where the relationship between Qatar and its neighbors witnessed tension following statements attributed to the Emir of Qatar and Qatar's claim that the website of the Qatari News Agency was hacked in May 2017, which made Qatar accuse Emirates of being behind the piracy, while Emirates denied that accusations. Qatar tended to enhance its electronic security in cooperation with America and Turkey, that crisis was reflected in the development of the crisis between Qatar and the Arab Quartet countries, namely Egypt, Saudi Arabia, the Emirates, and Bahrain by imposing a boycott, among its mechanisms was the blocking of websites funded and directed by Qatar that support terrorism.

The Arab region has also witnessed what is known as the growth of the phenomenon of electronic armies, which does not mean that this phenomenon has any military dimensions, but rather that it is a brigade trying to influence mutually by employing cyberspace in the conflict between the actors, in addition to the increasing vulnerability of the region to electronic attacks and piracy, especially in the Arabian Gulf, this prompted those countries to increase spending and investment in cybersecurity and to form national bodies for cybersecurity, like Saudi Arabia in November 2017, not to mention the presence of the Regional Cybersecurity Centre in the Sultanate of Oman with the support of the International Telecommunication Union[22]. The year 2020 also witnessed an increase in targeting countries in the Middle East: Thanos ransomware targeted several government institutions in the Middle East and North Africa region in July 2020, in a prominent example of employing data scanning tools to launch mysterious cyber-attacks. The hackers, known as MoleRAT, also used Middle East-related phishing messages to spy on a number of prominent government officials in the Palestinian territories, Emirates and Turkey[23].

International reports have estimated that the cost of losses related to cyber-attacks on infrastructure is expected to reach $265 billion by 2031, especially in light of the high rate of major ransomware attacks and malicious cyber-attacks that bring about several changes in operational technology, this industry needs to find fail-safe solutions to maintain the high throughput of these architectures safely and effectively. The complexities of the attacks have

[21] رويترز أرامكو" تتعرَّض لهجمات إلكترونية متزايدة عبر برمجيات خبيثة، الشرق ، فبراير 2020 ، https://bit.ly/3DOrEqW
[22] - الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، الموسوعة الجزائرية، الرابط، https://bit.ly/2J3GFua
[23] - الامن السيبراني في 2020 بين الفرص والتحديات والحماية، الموسوعة الجزائرية ، 2021، الرابط، https://bit.ly/3yGFWu8

increased and become more ferocious, and ransomware requests have now become fictional, as it is expected to exceed the cost of ransomware as a result of acquiescence and payment.[24]

- **Cyber threats in light of the pandemic**

The global scene of the outbreak of the Corona virus (Covid-19) also embodied the fragility of the global economic system and the weakness of the infrastructure of the facilities and institutions of health systems across the various countries of the world, as well as the weakness of the rapid response to combat that Covid and the inability to prevent its spread, which had serious repercussions and devastating effects on the global economy and the national economic and health security of countries. (Covid-19) had a serious impact on the criminal phenomenon through the decline of some traditional crimes and a significant increase in the rate of committing cybercrimes, especially cyber terrorism crimes on the infrastructure centers of countries, institutions and facilities, especially health ones.

As the commission of cybercrimes increased during the period of the outbreak of Covid-19 and the development of the means of commission as a result of the global closure policy and the shift to the remote work system, which imposed the use of security abbreviations with less supervision and fewer technical controls and many weaknesses in the cybersecurity system that the cybercriminal exploits to intensify his attacks on various sites, infrastructures, companies or sites for individuals. This is for the purpose of economic cyber espionage to steal (Covid-19) vaccine data by some countries or organizations, which can include data related to research proposals, drug development, manuscripts, virus testing, clinical trials, and drug manufacturing, which are estimated at billions of dollars for their scientific value and the intellectual property rights, especially with the increase in global investments in the health sector, which has harmed the global economy and the economic national security of countries.[25]

Thus, according to the above, electronic attacks affect a number of economic and social rights, the most prominent of which is the right for citizens to obtain public service through the state, in addition to the right to health care and access to clean water services and health care, it is worth noting that all these rights are protected by virtue of Articles of the International Covenant on Economic, Social and Cultural Rights[26].

[24] - 265 مليار دولار خسائر البنى التحتية جراء الهجمات السيبرانية، بوابة اخبار اليوم ، 31 اغسطس 2021، الرابط، https://bit.ly/3bPe9ie
[25] - الجرائم السيبرانية في زمن كورونا واثارها على الامن القومي الاقتصادي، الرابط، https://bit.ly/3urMBFZ
[26] ا لعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، مكتبة منسونا ، http://bit.ly/3aI7gKs

➢ Cyber-attacks, civil space and human rights

Human rights and civil society organizations, as well as human rights activists, are facing an increasing number of electronic attacks, such as phishing attacks and denial-of-service attacks, with the aim of taking revenge on them for their human rights work or forcing them to remain silent about various human rights violations, and this harms a number of civil and political in the International Covenant on Political and Civil Rights, including the right to form associations stipulated in Article 22 of the aforementioned Covenant, in addition to the violation of the right to privacy and freedom of opinion and expression.

In this regard, the website of the Syrian Network for Human Rights was subjected in October 2021 to unknown electronic attacks, which led the website to shut down for several hours. This matter is considered a continuation of the policies of treason and racism facing the organization that documents human rights violations in Syria of all categories. It is worth noting that some estimates indicate that the Russian government- backed groups are involved in this matter[27]. On June 17, 2019, a number of attempts were made to hack the accounts of the social media and email of the human rights organization PROMEDEHUM[28], a prominent civil society organization in Venezuela.

In the year 2018, with the start of the presidential elections in Azerbaijan, the government, with the help of affiliated groups, undermined the work of the opposing civil society organizations on the internet through a series of electronic attacks, as some human rights organizations' websites were subjected to direct denial of service attacks. Not only that, but some opposition media websites were hacked and all information available on them was removed. The Facebook account of Azerbaijani human rights activist Jamil Hasanli was also hacked and all his followers were deleted[29]. In Vietnam, civil society organizations and activists were subjected to takeovers of their electronic accounts, through the use of cyber-attacks based on fake and malware-laden bots that violate the digital security of the Internet user to access their private account information[30].

Accordingly, it can be said that the requirements for the availability of international cyber security against cyber-attacks and threats are to ensure the safety of electronic defenses, and that they are not exposed to any emergency technical defect, and

[27] الشبكة السورية لحقوق الإنسان تتعرض لهجمات إلكترونية، شبكة أرام الإعلامية ، https://bit.ly/3n1oI3r
[28] https://bit.ly/30mnKan. Frontlinedefenders. CYBER ATTACKS AGAINST HUMAN RIGHTS ORGANISATION PROMEDEHUM
[29] https://bit.ly/3BPHyAP،February 2018،meydan،Azerbaijan's authoritarianism goes digital
https://bit.ly/3BPHyAP،February 2018،meydan، Azerbaijan's authoritarianism goes digital
[30] .Ccessnow . Vietnam under review at the Human Rights Council: Cyber attacks on civil society a key concern
https://bit.ly/3FLBv2C

that this issue is not dealt with separately from others, but within a comprehensive defense arsenal that constitutes a deterrent framework for any preemptive war, which is what The international community is required to focus on the relationship between cybersecurity and issues of economic and social development and political stability, to formulate an international strategy to confront the escalation of electronic dangers, the importance of the cooperation of all actors in the global information society to establish a global culture of cybersecurity, and the importance of balancing security considerations and the freedom to use cyberspace and what Between the global monopoly of technology and its transmission in the countries of the world.

Then, **Maat for Peace, Development and Human Rights** asserts that no country or institution in the world can achieve 100% cybersecurity, because we are in the world of technology struggle, so it is no longer appropriate to say that today's technology can be hacked by tomorrow's technology, but rather the fact that the world Every second of a new technology penetrates and undermines what preceded it, but the risk of threat and cyber-attack can be significantly reduced to a level that allows us to continue to benefit from the vast opportunities offered by digital technology. The Corona pandemic also showed that all countries of the world must realize the unity of the common destiny on this planet, and that they will not survive alone in light of the imposition of a policy of isolation and individualism and the weakness of global partnerships, and that there is no way for them to solve these crises and pandemics except for everyone to meet around the round negotiating table, to accelerate getting out of the crisis to enhance international cooperation and reset global partnerships, to facilitate recovery and rebuild social, economic and health systems in comprehensive and sustainable ways and help prepare for future risks and epidemics in the interest of all countries.

Maat also affirms that the conclusion of the agreement in this regard in the future will mean moving individual criminal responsibility for supporting, training or financing any armed groups that could use electronic means for non-military purposes against other countries. Therefore, the countries must reach a compromise in order to take such measures, to protect its safe access to cyberspace and the services it provides.

Hence, Maat recommends the following:

1- The importance of the need to open the way for fruitful cooperation between governments, individuals and companies working in communication and information technology, in order to enhance the role of cyberspace in economic growth, improve the lives of citizens, freedom of opinion and expression, and promote tolerance between cultures

2- The need for urgent and concerted international efforts to confront cyber security threats with the possibility of working to resolve conflicts on the ground to prevent their transmission.
3- Work on the compatibility of laws related to cyber conflict with international law and the importance of international initiatives to protect cyberspace as well as research and development in the field of defenses against electronic dangers and strengthening forms of international cooperation in order to combat them in order to enhance the security of cyberspace as an international facility and a common heritage of humanity.
4- The need to take new measures regarding a periodic cybersecurity review of the international dimension associated with crypto assets, as crypto assets are by their nature cross-border in their applications and infrastructure, in addition to the rapid development and complexity of those crypto assets.
5- There must be a continuous evaluation of the legislation issued to verify that it can be applied effectively to this type of assets or whether it needs amendments or guidance.
6- Measures must be taken to enhance the capacity of criminal justice agencies in digital investigations, and to ensure that they have the appropriate tools, techniques, skills, artificial intelligence, big data, and high-performance computing in security policy, all of which represent an essential priority for achieving cybersecurity, and then combating cybercrime.
7- The need to invest in the field of cybersecurity and establish international partnerships with leading and developed countries in this field to share information about the cyber threat to define the parameters of the global development of cyberspace, and to establish new centers of cyber innovation to create a complete system to protect cyber security and to raise the capacity to combat cyber-crimes.
8- Countries must work to increase spending on developing capabilities in the field of cyber defense, and allocate resources in the state's general budget, or in its security and defense budget, in addition to forming councils concerned with developing policies related to cyber security as one of the tributaries of national security.