Cyber Social Disruption due to Cyber Attacks

Jorge Barbosa
Coimbra Polytechnic Institute, Portugal

jorge.barbosa@isec.pt

Abstract: We analyze the implications of cyber war actions directed at specific targets, such as critical infrastructures, for modern civil societies that are profoundly dependent on computer systems. These critical infrastructures, whether they are cyber-physical systems or computer systems can be paralyzed or even destroyed if the systems used to directly or remotely manage them are cyber-attacked. Cyber-attacks in the context of cyber war, can generate chaos, which combined with the domino effects caused by the impact on other computer systems, then those directly attacked but indirectly affected, can theoretically lead to major disruptions to the internal order, or even to civil war, due to the scope that such actions may reach. The disturbances caused in civil society as a whole, and in military structures and equipment can go far beyond the local effects on the targets attacked, as would happen in a conventional kinetic war action. The crisis and social disturbance caused may even put the sovereignty of the attacked state at risk. For this specific case of social disruption, which is caused by cyber war actions, we use a concept to describe the situation more adequately, which we call *Cyber Social Disruption*.

Keywords: Cyber Social Disruption, Cyber Dependence, Cyber Warfare, Critical Infra-Structures Protection

1. Introduction

It is considered that in the event of a conventional war, the protection, through conventional kinetic means, of infrastructures is essential. In the event of a cyber war, those structure's protection is also fundamental, due to the local and systemic effects that may indirectly occur on other computer or cyber-physical systems, other than those attacked. Physical protective barriers may be useless in the event of a cyber-war, making cyber barriers indispensable.

Another important aspect, that difficult the establishment of protection against cyber-attacks, is that those protections must be thought out, designed and implemented during peacetime. The speed and unpredictability of a computer attack won't allow time for the cyber protection equipment to be built, put into operation, and used, with the required training. In the case of a conventional kinetic attack, all, or part of the conventional kinetic defences need to be installed close to critical infrastructures, such as the placement of anti-aircraft missile systems next to dams, and may be installed with relatively little advance, due to the fact that kinetic warfare actions are more visible and predictable, through on site-intelligence or remote observation such as satellites, allowing protective actions and defence measures. On the other hand, actions in cyber-war can take place in total secrecy, and be a total surprise for the attacked country.

In the event that a cyber-attack has been launched, it may be too late to implement cyber defence actions, due to the speed and unpredictability of the action. Computerized control systems may immediately be destroyed or rendered unusable, by the deletion or scrambling of database records related to industrial, financial, logistical, or energetically related systems. The result may be the total disruption of energy, including fossil fuels and electricity, food distribution logistics, or even drinking water production and distribution.

Likewise, unlike conventional kinetic protection systems, the effective lack of knowledge of one's own, and the enemy's computer systems, their constant evolution, and the evolution of the cyber techniques affecting them make it very difficult to develop and implement effective protection mechanisms promptly. What is installed today may no longer be effective tomorrow.

2. Scope of this work

The consideration of the cyber actions that we intend to make in this paper does not exactly focus on common cybercrime actions normally carried out by individuals or organizations of individuals against institutions or individuals, in most cases to obtain economic benefits from their actions. These actions are also isolated acts in the sense that they can be triggered simultaneously against several institutions or people but are not usually carried out in a coordinated manner and with the aim of causing a major impact on the society or country attacked as a whole. We will therefore consider actions that are not specifically directed at individuals or institutions in themselves but that actions against these institutions in particular against their computer and/or cyber-physical systems, usually referred to as critical infrastructures, which operate are done in a coordinated and systemic aim having as its objective as a whole and in the coordinated and specific way in which the paralysis of a society or some of its main sectors are triggered through the total or partial destruction of these critical systems or their paralysis and not the obtaining of simple economic benefits but yes with political, economic or military objectives against a country to affect their sovereignty. Therefore, and also taking into account these

objectives, this type of cyber-attack is, specifically, called cyber war action. It is assumed that those behind these cyber actions are other countries interested in disturbing the attacked country.

These actions and effects are not new, for some years now reports of actions against computer systems and cyber-physical systems have been made. Many of these reports could not be factually proven as they were mostly secret actions or habitually denied by their likely authors and even by the target countries themselves, strange as it may seem as they cannot or do not want to confirm these attacks that they were targeted in order not to expose secrets or show weakness. These cyber war actions are often launched using techniques commonly used in common cyber-crime, but their final objective is not the same as mentioned above. It is also assumed that they are not perpetuated by individuals or groups of individuals acting on their own, but by organized groups created or at least dependent on the perpetuating countries organized as cyber-attack military corps of those countries, *Cybercorps*. These cybercorps, both cyber defense and cyber-attack, are even considered, given the great importance assigned to them, as the 5th military operational domain designated as "*Cyberspace"* alongside the three more traditional operational domains "*Land*", "*Sea*" and "*Air*" and the also relatively recent fourth operational domain, the "*Space*".

As early as 1993 in the RAND Corporation publication "*CyberWar Is Coming!*", the authors used expressions such as "*As an innovation in warfare, we anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century.*" and also "*Netwars are not real wars, traditionally defined. But netwar might be developed into an instrument for trying, early on, to prevent a real war from arising.*", (Arquilla & Ronfeldt, 1993).

Figure 1 - Cover of TIME magazine of August 21, 1995: Cyber War

Time magazine also dedicated its cover to this topic on August 21, 1995, Figure 1. The advent of Cyberwar was 25 years ago. The USA then created what was considered the first "*Cybercorp*", the "*Air Force – 1st Cyber Division*", Figure 2.

Figure 1 - Air Force – 1st cyber division

In addition to this difference in actors participants in the actions that we mentioned and the techniques similar to those of ordinary cyber-crimes, a big difference lies in the fact that these Cybercorps maybe they use more sophisticated means based on computer flaws not yet publicly known and called “Zero Day Vulnerability”, ZDV from which they are created cyber-attack software. This software is called Exploit and if it is developed for a ZDV it will be called “Zero Day Exploit”, ZDE. ZDEs are the most powerful cyber weapons because as they are based on a computer flaw still unknown to others, there is, a priori, no cyber defense for them.

The approach considered in this work then results from the assumption that it is necessary to go a little further than what is usually considered when addressing common cyber security topics and enter into a broader approach, including considerations related to cyber war because its consequences are much more pernicious.

In other words, the means involved and the possible actions are not simple cyber security acts but much more planned, sophisticated actions, foreseen in advance with a view to possible future use in the aforementioned contexts, these are true acts of war but triggered without being through of the usual kinetic weapons. As such we think that a different framework and importance must be given to acts due to cyber war actions in contrast to that attributed to simple cyber-crime actions, hence the need to systematize concepts in order to be able to perceive more coherently and correctly its results. In particular, we are concerned with making such a systematization in terms of its effects on civil society, namely the social disruptions that it can and we understand that they will cause.

There have been articles for some years now that address this topic of cyber security attacks with possible effects on civil society, for example (Lena Yuryna Connolly, 2020), (Cartwright, 2023), (Erik Schrijvers, 2021), and (V. Palleti, 2021). But from the analysis of these papers that we did, their focus is not on systemic and coordinated actions triggered by countries through their already mentioned organized structures, the Cybercorps or similar, but rather and generally framed in “common” cybercrime actions which alone can also cause social disturbances but with much more limited effects in time and space and much less dangerous.

These possible disruptive actions for civil society caused by these acts of cyber-crime are not in themselves their objective but rather something that in the military context is usually called side effects since the objective of cyber-crime is, as already mentioned, normally the obtaining economic benefits; cyber war actions may have exactly the opposite objective, that is, to cause this disruption of civil society.

Then, such actions, although they can be disruptive, are not or presumably will not be comparable in their effects and disturbances resulting from attacks in the context of cyberwar in which the vector of social disturbance in the society of the attacked country would be one of the main vectors considered and of much greater dimensions and proportions. Since 2018, we have worked in this area of cyber war and its effects at various levels, including social disruption, for example (Barbosa, 2020), (Barbosa, 2022), and (Barbosa, 2020). However, the systematization and definition of concepts, namely those relating to acts arising from actions of cyberwar that affect civil societies is fundamental, given its danger and possibility of being considered in acts of cyberwar. This conceptualization is also necessary to differentiate it from the acts of vulgar cyber-crime.

3. Use of Cyber Weapons

The usage of cyber weapons is possible due to the weaknesses created by the existence of hardware and software vulnerabilities, which, generally, all computer systems have. When those vulnerabilities are known by a restricted group, but not publicly known, then are called *Zero-Day Vulnerabilities* (*ZDV*). *ZDV* can be used with great advantage in the construction of applications called *Exploits*, which if based on *ZDV* will be called *Zero-Day Exploit*, *ZDE*, which can be used with great success as cyber weapons. These *ZDEs*, by exploiting vulnerabilities in computer systems, can take control or even paralyze systems affected by these vulnerabilities. If those systems are linked to the control of so-called *Critical Infrastructures*, their affectation and even their shutdown or destruction can harm the attacked country and the normal life of society in that country.

The interest in this type of cyber weapons is not only its usage in common cybercrime, but also in war actions between sovereign States against other sovereign States. As this type of actions can compromise the sovereignty of a State, they are called cyber war, instead of cyber security actions, a term used regarding common cybercrime actions.

From industrial process controllers, such as the very well-known SCADA - Supervisory Control and Data Acquisition or the PLC - Programmable Logic Controller which are industrial controllers of legacy systems with consequent deficiencies due to being based on not only old technologies but mainly designed at a time when there were not so many security concerns, particularly at a time when the internet was not yet massively used nor were they originally designed taking into account the necessary security concerns subsequently taken into account. Despite this, these controllers are still widely used today and due to great difficulties if not even impossibility of replacing it and are currently still widely used in critical infrastructure control systems, such as dams, other power generation stations, water treatment and supply systems, transport logistics, fuel logistics, etc., up to sophisticated cyber-physical systems and also sophisticated computer systems linked to databases, whether for customer relationship management or financial systems in banking services, public or private institutions, ATM systems or automatic payment systems, practically everything is based on computer systems, with the known benefits arising from their use. The disruption, destruction, and alteration of those systems can paralyze, or seriously affect modern societies, due to their dependency on them.

The opposite side of this beneficial use is that if such systems are insecure and therefore possibly penetrable, they can result in catastrophic effects, since the disruption of the aforementioned systems, their destruction or alteration can paralyze or seriously affect modern societies. Therefore, this dependence is critical from this point of view and therefore these systems are tangible targets and subject to military actions against them. These military actions can be triggered by conventional kinetic means, but also triggered by computer systems, through so-called cyber weapons. These cyber weapons act directly on the enemy's computer systems, destroying them, paralyzing them or altering them in such a way as to interrupt or interfere with the normal functioning of the equipment they control or manage.

The theoretical possibilities offered by this military option lead a large number of countries, other than conventional powers, to consider its use. Theoretically, the amount of resources needed, human and material, are much lower than those needed to launch conventional military operations. Although the economic and human resources necessary to acquire these technological skills means may be considerable, they are exceptionally lower than those needed to train and equip human resources in conventional kinetic war. The combination of these factors makes this option very desirable and, theoretically, may lead to the proliferation of cyber powers prepared for cyber warfare, as an alternative to kinetic warfare, (Barbosa, 2020).

4. Protection of Cyber-Physical and Digital Critical Services

Concerning cyber protection of services and infrastructures, it must be kept in mind that systems can only be cyber-attacked if they are a priori predisposed to. Flaws must be present in the systems to allow the use of Exploits, which take advantage of those failures, they interfere with the normal functioning of the systems. Therefore, protection actions must be focused on two vectors, (Barbosa, 2019):

1. Eliminate these eventual failures;
2. Obviates the possible use of ZDV.

To protect these vital installations, the Cyber Defence actions necessary for this protection may involve not only direct actions triggered during cyber-attacks but essentially depend on indirect actions that, as already mentioned, were studied, planned and implemented in time.

Three large groups are considered, listed below and we will detail:

4.1 Critical and Essential Conditions for Cyber Defence

1. Legal and Organizational Frameworks
2. The Human Factors
3. Technological Needs

4.2 Cyber-Permeability of Systems and Infrastructures

1. Obsolete Software or Hardware
2. Alarmist
3. System Operators
4. Technical Support Team
5. External Exposure
6. Networks Interconnections
7. Physical Means
8. Physical Access of People

4.3 Commitment to Cyber Means for Cyber Defence

1. Chain of Command
2. Hierarchical Communication Protocols
3. Rapid Integrated Response Teams
4. Replacement Equipment

The first group includes cyber defence actions that all countries must take to protect their critical services and infrastructure. These actions must be general, and not specific for the protection of any particular facility. The creation of possible cyber armies with the mission of triggering defensive and offensive cyber actions, after an attack is initiated, is applicable here. The creation of a cyber-army can be a disincentive to the usage of this type of attack, by other states. Also included at his point, are the equipment and technological resources that allow these cyber armies to carry out cyber defence actions.

In the second group of cyber defence actions for critical services and infrastructures, we consider the equipment itself, that is, the software installed and in use, and the hardware used in the computer systems for command, control, or management of these services and infrastructures. It must be a priority that all software used is fully updated and certified, Periodic routines must be established to check the existence and respective installation of updates for the applications in use, including the basic operating systems or the exploration and control applications themselves. If any of this software is subject to constant updates, this situation should be analyzed and its replacement with other equivalent software should be considered, as constant updates may be a sign of fundamental problems in the software in question. The equipment that is being controlled must also be monitored and analyzed. We must not only specifically focus on the hardware and software of the computer control systems, but also have a more comprehensive perspective including the equipment itself that is being controlled. It may be that problems in these controlled equipment are caused by alteration or physical destruction through the actions of the computer systems that control them.

Special attention should be paid to the operators of these systems, namely by providing them with constant and appropriate training, not only in technical aspects but also in awareness and responsibility. These operators can be the weak party when it comes to the security of these systems and infrastructures. They must be deeply aware of the need to have and adopt a total, integrated and holistic security awareness. Small details about the actions they can take can have major consequences on the overall security of the systems they operate, such as the password policy they must have and use. In this sense, passive and active security protocols must be established and strictly followed.

The technical teams supporting the operation and management of these services and infrastructures must also be aligned with these needs and procedures. Concerns should not only be related to technical aspects, such as maintenance, but on the contrary, they should have a systemic approach.

Exposure to external action should be a major concern. Those external actions can have different origins. Computer networks must be carefully monitored and examined. Connections to networks of any type should not be permitted, except those strictly necessary for the operation of the systems, particularly their remote operation. It should not be forgotten that, as already mentioned, many of these infrastructures still use *SCADA* and *PLC* controllers. These controllers, particularly those from the first generations, were designed at a time when, in addition to security issues being less pressing and known, the systems for which they were designed were not at the time connected to a network, namely to the Internet. For various reasons, most of these systems

were subsequently connected to the Internet without themselves and the subsystems they controlled, namely the controllers, having been updated. Whenever possible, there should be a complete separation between public access networks and private access networks to these services and infrastructures.

The physical means used must also be subject to special care. Consideration should be given not only to devices that can be physically connected to systems via computer networks but also to any device, such as pen drives, floppy disks or *CD-ROMs*, that can transfer, purposely or not, harmful applications that interfere with normal functioning of systems. It must also be taken into account that the devices that connect to the IT systems controlling these services and infrastructures must not only be reliable but above all trustworthy. In the literature there are several references to situations in which it is suspected that common computer peripheral equipment, for example printers, have been used to transport *Exploits* to the facilities that later passed into the processing systems, infecting them so that someone from the outside could take over the control of such systems. There are suspicions that the use of such *Exploits* in some cyber wars, for example the attack known as *Stuxnet* or the eventual cyber-attack to interfere, blinding them, with Syrian radar systems before an air attack, was possible using as a gateway input for cyber-attack computer peripherals, (Zetter, 2014), (Carr, 2012) and (Clark & Knake, 2010).

Physical access by unauthorized people to service facilities and critical infrastructures must be prohibited not only to avoid triggering direct actions, even kinetic ones but also because they may intend to install applications that trigger cyber-attacks on the IT systems of these infrastructures and therefore this access should never be allowed.

The speed and unpredictability associated with a possible cyber-attack are not conciliable with the delays in the chains of command of the command structures involved in triggering and conducting defensive cyber actions, whether to minimize effects or launch cyber counter-attacks. Therefore, chains of command and respective communication protocols must be very well defined and established so that there are no failures or delays that could lead to the impossibility of minimizing effects and taking countermeasures. Another aspect to consider is the creation of integrated response centers for cyber warfare actions.

The issue of replacing equipment is one of the most critical aspects of these *Cyber Defence* actions. Considering equipment replacement as an act of *Cyber Defence* is related to the issue of rapid equipment replacement.

This energy replacement can also be considered a defence action because it can allow the effective launch of actions to minimize effects and cyber-attacks, which could be impossible, for example, if there is no energy. However, as mentioned, it is one of the most critical and difficult aspects to achieve.

As can be seen in the simulated example of the destruction of this type of equipment within the scope of *The Aurora Generator Test*, (Clark & Knake, 2010), the eventual physical destruction of electrical generators in a dam is possible. Replacing generators may not be able to be done quickly given the uniqueness and specificity of this type of equipment. Its replacement, if we consider the production time, transportation, and installation time as well as the tests necessary for its effective entry into operational service, can take months. However, the country or a large area of the country may be deprived of electricity from this source. Other similar examples, considering other types of critical equipment, could be considered with the same restrictions.

5. Real Effective Cyber actions against physical targets

There are examples of experimental actions of real physical destruction, simulating software installed remotely on computers that control generators in hydroelectric plants, in which it was relatively easy and quick to physically destroy one of their generators. An example of this is the experience of the *US Department of Energy*, which launched a national *SCADA* testing program in 2003 at the *Idaho National Lab*, *INL*, called the *Aurora Generator Test* and carried out in this laboratory, (Zetter, 2014), (Clark & Knake, 2010).

It was shown in Figure 3, that it was easy and quick (Singer & Friedman, 2014) to destroy a generator similar to those in American dams. In the event of a similar real action, orchestrated as an act of cyber warfare, a country's energy production system, or part of it, could easily be disrupted. In the pictures of Figure 3, we can see that the generator is releasing smoke due to the high rotations to which it is being subjected due to the action that simulates a remote control attack on that generator and ends up self-destructing, (Singer & Friedman, 2014).

Figure 2 - Aurora Generator Test, Idaho National Lab, INL

Another action, not experimental, but real, which became known as *Stuxnet*, the name of the main malware used, was launched against facilities at the *Natanz Nuclear Complex*, in Iran, (Zetter, 2014), (Singer & Friedman, 2014) and (Clark & Knake, 2010). Many authors consider this action as the first real action of an act of cyber warfare. The centrifuge operations of this complex were severely disrupted and some of the centrifuges were physically destroyed. The action was carried out by introducing, into the computers that control the centrifuges *PLC* controllers, an *Exploit* that was later called *Stuxnet*.

On April 27, 2007, cyber actions were launched in the form of violent *DDoS* attacks, which targeted several computer systems in Estonia, namely important websites of the government, parliament, banks and the communications system in general, which resulted in known as the "*Estonian Cyberwar*". It is assumed that for these *DDoS* attacks, a bot net consisting of 85,000 servers was created, with the attacks lasting three weeks and sixty websites being attacked. These cyber actions have never been officially attributed to any country. However, the Estonian Foreign Minister attributed the attacks to Russia, which has always denied its official participation in them. Russia considered the actions of individuals who acted as "*Patriotic Hackers*". One of the theories is that they were triggered by the Nashi movement, "*Ours*". It is believed that this group was organized by supporters of the pro-Putin regime to carry out actions against anti-Motherland forces. Its leader was an advisor to Russian parliamentary leader Sergei Markov (Singer & Friedman, 2014).

These cyber-attacks on Estonia reinforce the conviction that it is difficult to correctly determine the identity of cyber attackers. It is estimated that 25% of the attacks (Singer & Friedman, 2014), presumably originated from computers located in the USA, a country that was an ally of Estonia, and that for this reason and others, theoretically, would have no interest in carrying out such an attack. attack.

At the height of events and due to the near paralysis of its country, the Estonian government requested help from allied countries and organizations, namely NATO, invoking Article 5 of the *Collective Self-Defense Agreement*.

In the 2008 Russia-Georgia War and due to events in Georgia and South Ossetia, cyber-attacks against Georgia occurred. They were highly coordinated among themselves and linked and coincident with invasions by land, sea, and air.

Previously, in the second Russia – Chechnya war that took place between 1997 and 2001, there are reports that the FSB, the Russian Federal Security Service, was responsible for the attack and takedown of Chechen government websites at the time.

Cyberattacks against Ukraine were allegedly launched by Russia in retaliation for that country's actions in Crimea and Donbass. Malware called *Petya* was used and electricity companies, ministries, banks, and newspapers were affected, (Farmer, 2018).

There are suspicions of the Chinese government's involvement in cyberwar actions, disguised as the actions of "*Patriotic Hackers*". In May 1999, a NATO plane accidentally bombed the Chinese embassy in Belgrade. The Chinese Red Hacker Alliance then launched cyber-attacks against US government websites.

Another action reportedly took place after an accidental collision between an American military plane and a Chinese one in the South China Sea and in protest Chinese hackers launched cyber actions, allegedly in self-defense, against US government websites and institutions. The newspaper The New York Times even classified these actions as those of the First World War via the Web, "*World Wide Web War I*".

In 2009, North Korea launched cyberwar actions and *DDoS* attacks on a small scale and in specific contexts against the USA on that country's National Day.

Another action attributed to North Korea took place in 2014. Although it is not a cyberwar action, we mention it to highlight and accentuate the scope and the most varied forms in which these attacks can take place. The action was taken against Sony Pictures Entertainment's computer system. The North Koreans felt that their country's honor was offended in the film "The Interview", where the country's leader was allegedly portrayed pejoratively. It will have caused Sony 100 million dollars in losses.

In December 2008, after a military operation launched by Israel, "*Operation Cast Lead*", several cyberwar actions took place between Israeli and Arab hackers.

Reportedly, there have also been cyber warfare actions in the current conflict between Ukraine and the Russian Federation. However, the cyber-attacks referred to in this paragraph had more the objective of preparing and conditioning the kinetic actions that followed, in what in military strategy is called shaping the theater of operations, than being total cyber war actions, even if inserted in a global action as one of the components of a hybrid war.

6. The Cyber Social Disruption Concept

As far as conventional wars are concerned, on a primary level, the military and political strategists and leaders of a country equate the potential, in the face of a possible and determined enemy, through two factors: the "*Attack Capacity*" and the "*Defence Capacity*" of both their country and that of the enemy country. Considering these capacities, in the case of conventional war between these two countries, infers who, theoretically, can become the winner or the loser.

In the case of a *Cyber War*, these considerations must be different, given the much more complex scenarios.

Mutatis mutandis when considering the strategic analysis of similar factors in a *Cyber War*, the key factors to consider should not only be the two mentioned above, but a total of three, namely: "*Cyber Attack Capability*", "*Cyber Defence Capacity*" and a third and another factor, concerning conventional war, the "*Cyber Dependency Capacity*" of the countries involved, (Barbosa, 2018).

We consider the *Cyber Dependency Capacity* of a country as the dependence that this country and its society have on IT and the complexity and density of connections and interoperability between its IT systems. The larger the organization, complexity, and density of connections in its IT systems, the greater the country's dependence on IT will be. The greater this dependence, the greater the vulnerability of that country to possible failures in its IT systems. A serious computer failure in an important critical computer system can be a big problem and, in extreme cases, even paralyze the country or many sectors, (Barbosa, 2020).

Modern and developed Western societies, as well as those in some Asian countries, have a very high *Cyber Dependency Capacity* and as such are extremely sensitive to problems in their computer systems, particularly those resulting from *Cyber War*.

Less developed societies are also often underdeveloped in terms of the massive use of information technology in the various organizational aspects of their society. This means that they also have a very low *Cyber Dependency Capacity*. As they do not rely heavily on IT for their daily operations, they are not as sensitive to IT failures and may not even have IT "targets" to attack.

The benefits for civil societies in countries resulting from the massive use of information technology in all aspects of that society, namely service provision, government, central and local administration, banking and finance, transport management, logistics, food, and fuel distribution, etc. it is today an indisputable reality in all minimally developed countries. It can even be said that it is currently no longer possible for these countries to survive without the means and facilities provided by the information society.

Maintaining the information society and the means necessary for its functioning is extremely important. Its alteration or destruction is unthinkable in the current development context. Actions, even relatively small and isolated in their scope and effects, such as the acts of hackers, who, individually or in small groups, trigger cyber actions against individuals or companies, can have relatively serious consequences, (Singer & Friedman, 2014) and (Carr, 2012).

A concern that many security and defence agencies and services have is that such acts do not come from these actors, but are orchestrated and triggered by other actors, namely countries, which, for this purpose, constitute specialized units. If concerted and large-scale actions are carried out against any country, through the exclusive use of IT means, they could profoundly affect the IT systems of that other country, particularly those linked to its critical infrastructures.

This ability of a country's cyber dependence to be directly linked to that country's involvement with information technologies, in particular with the greater or lesser degree of development of its information society, can also transform them into preferential cyber targets.

The combined effects of cyber actions can be so great and disruptive to the experience of civil society in the attacked country that they can lead to serious disruptions in that country. These service dysfunctions, namely the logistics of supplying food, electricity, water, fuel, and other essential goods, banking services, and the impossibility of obtaining money from *ATM* systems or similar, could create not only disruptions in the experience of civil societies but a total disruption. We call this specific type of disruption as *Cyber Social Disruption*.

7. Conclusion

The use of cyber weapons, which allows the launch of *Cyber Wars*, is possible due to vulnerabilities in computer hardware and / or software, which, in general, all computer systems have. When these failures exist in systems more directly related to civil society, for example, critical infrastructures, the consequences of the negative effects of cyber-attacks can be very disruptive to the normal life of civil societies.

In the case of a *Cyber War*, this could lead to a situation that we consider a concept to take into account in *Cyber War* situations and which we call *Cyber Social Disruption*!

Concerns about cyber wars are great because they can be used to totally destroy the target country, both physically and logically. *Cyber Social Disruption* can lead to chaos in modern societies, resulting from the combination of cascading cyber effects, which can consequently cause turbulence and severe disturbances in internal order, and even lead to civil war.

References

Anon, n.d. NATO Cooperative Cyber Defence Centre of Excellence. [Online], s.l.: s.n.

Barbosa, J., 2018. Pequenas potências militares convencionais, Grandes potências militares cibernéticas - Abordagem da utilização de meios informáticos na defesa/ataque militar moderno, Lisboa: Portuguese National Defence Institute, IDN.

Barbosa, J., 2019. The ZDEs as cyber weapons. La Toja, Galicia, Spain, s.n.

Barbosa, J., 2020. Cyber Humanity in Cyber War. Chester, UK, s.n.

Barbosa, J., 2020. Cybernetic Dependency Capacity. In: R. a. others, ed. Developments and Advances in Defence and Security. Smart Innovation, Systems and Technologies. Singapore: Springer.

Barbosa, J., 2020. Is Cyber Warfare an Alternative?. In: Á. R. a. R. P. Pereira, ed. Developments and Advances in Defense and Security, Smart Innovation, Systems and Technologies . Singapore: Springer Nature.

Barbosa, J., 2022. How to Educate to Build an Effective Cyber Resilient Society. In: I. Global, ed. Research Anthology on Advancements in Cybersecurity Education. Hershey(Pennsylvania): Information Resources Management Association, p. 578.

Caldas, A. & Freire, V., 2012. Cibersegurança: das Preocupações à Ação, Lisbon: Portuguese National Defence Institute.

Carr, J., 2012. Inside Cyber Warfare. Second Edition ed. Sebastopol, CA, USA: O'Reilly Media, Inc..

Cartwright, A., 2023. The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing, Volume 37.

Casimiro, S. d. V., 2018. Quadro Legal para a Cibersegurança e a Ciberdefesa. In: IDN, ed. Contributos para uma Estratégia Nacional de Ciberdefesa. Lisboa: s.n.

Clark, R. A. & Knake, R. K., 2010. Cyber War: the next threat to national security and what to do about. New York: HarperCollins Publishers Inc..

Erik Schrijvers, C. P. ,. R. P., 2021. Preparing for Digital Disruption. s.l.:s.n.

Farmer, B., 2018. Russia was behind 'malicious' cyber attack on Ukraine, Foreign Office says, s.l.: s.n.

Lena Yuryna Connolly, D. S. W. M. L. B. O., 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity, Volume Volume 6, Issue 1.

Ranger, S., 2018. What is cyberwar? Everything you need to know about the frightening future of digital conflict., s.l.: s.n.

Singer, P. W. & Friedman, A., 2014. Cybersecurity and Cyberwar - What everyone needs to know. N. Y,: Oxford University Press.

V. Palleti, S. A. V. M. e. a., 2021. Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecur 4, 8.

Zetter, K., 2014. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon". N.Y.: Crown Publishers.