The definition of a cyberweapon

João Carlos Leandro da Silva

Via Medole 22, Castiglione delle Stiviere (MN), Italy

Cyberweapon or cyber-weapon but does it matter how we write it? Yes, it does! Everyone knows that words are essential when it comes to naming anything that human beings seek to understand. In fact, finding the correct word to describe an object or idea is of vital importance to both written and oral communication. For instance, Marie Curie (1867 – 1934) was the first to coin the term "radioactivity" which was fundamental to the development of this scientific area. Consequently, my attempt to define "cyberweapon" will consist in a deep analysis of the words "cyber" and "weapon". Please note that I will constrain myself only to its technical side. Strictly speaking, I will not try to deal with its legal and strategic aspects [1] because such is beyond my competence. My goal is to delineate a rigorous path whereby anyone can determine if a given entity is or is not a cyberweapon. The aim of this paper is to discuss the subject at hand as clear and concise as possible in order to reach a wide audience.

1. VIRTUAL WORLD AND REAL WORLD

On 29 October 1969, a communication link on the Western coast of the USA was able to transmit and receive two single letters ("L" and "O") between two distant computers. Soon after other machines joined in and within a few decades, millions of devices and users shared information via a network of local and global networks. The data exchanged was truly massive and it continues to grow at an incredible rate until this very moment. Today such network is the World Wide Web or simply Internet. Here, we will refer to it as the virtual world that consists of two layers. The top layer is the surface web while the bottom layer is the dark web or deep web. The first is that portion of the Internet that is available to any user with a typical browser such as Firefox while the latter is only accessible to those with a special browser known as TOR (The Onion Router). Those users that surf the Internet with TOR are practically anonymous in every sense of the word whenever they access a given website. Accordingly, in the virtual world an individual can play any role he/she desires and may or may not get away with it. The same is not true in the real world. For example, if you are a man but pretend to be a woman and decide to enter the ladies bathroom, do not be surprised if someone yells or calls the police. In essence, in the real world you are not anonymous because others can see, hear, touch and smell you. There is no doubt that if someone wants to hurt another person, it is much easier to accomplish such in the virtual world rather than the real world.

2. STANDARD WEAPON

The word "weapon" brings to mind the firearm of a policeman, the riffle of a hunter or the machine gun of an army soldier. But a kitchen knife or a car is also weapon, so how can we define it? Conventionally, a weapon is any object that may hurt or kill a person or an animal. It may also damage or destroy other objects. Since a person may kill with bare hands, here we will not consider the human body as a weapon itself. Other exceptions are natural catastrophes (earthquakes, tsunamis, etc) and unintentional actions like a vase falling (as a result of a storm) from a balcony and striking someone or a car that is parked downhill and due to a mechanical problem of the brakes starts to move and hits a pedestrian crossing the road. Therefore, we assume a weapon to be some type of tangible matter with the potential to kill or destroy coupled to a deliberate human intervention. At this point, it is clear that conventional weapons can vary both in size and form ranging from a simple bullet to an aircraft carrier. These include any sort of machine such as a drone or a tank and even fully automated vehicles. The important thing to realize is that a standard weapon belongs to the real world and exists as a physical object.

3. LAND, SEA, AIR AND SPACE

Throughout the ages, mankind has always been in conflict for one reason or another. As science progressed so did the military technology. In medieval times, fighters using swords and spears fought on land. A century later, ships called galleons (multi-decked sailing ships) with many cannons dominated the seas. In 1794, the French used hot-air balloons as aerial observations posts in the Battle of Fleurus. Note that in this specific case, the object itself (balloon) did not kill or destroy but the information it gathered from the air provided the French ground forces with strategic advantage culminating in victory. In conclusion, an apparently innocuous balloon in the sky resulted in a decisive weapon after all.

The First World War (1914 – 1918) saw the inclusion of technologies such as the telephone and new weapons like submarines and fixed-wing aircraft. Furthermore, this horrific global conflict employed chemical weapons for the very first time in history. Chlorine and mustard gas were responsible for the deaths of many soldiers and civilians. Things got much worse in the Second World War (1939 – 1945) with innovative weapons as bombers, aircraft carriers, anti-tank guns, mines and rockets like the infamous V-2. Once again, scientists were able to develop nuclear weapons withholding a destructive power never seen before. In fact, the combined death toll from the bombings of Hiroshima and Nagasaki was many thousands of lives between civilians and military personnel. Besides, new types of biological weapons (insects) were developed and put into action during WWII. Both nuclear and entomological warfare were not standard weapons but weapons of mass destruction. On 4 October 1957, the Soviet Union successfully launched a satellite into orbit. Such achievement started a space race because the following year, the USA did the same. With the rise of ICBMs or intercontinental ballistic missiles both nations developed new space weapons such as reconnaissance satellites and anti-satellite technology. When an ICBM flies from the Earth into space and then reenters, an opponent can try to intercept it in three different ways: ground-to-space, space-to-space and space-to-ground.

4. CYBERSPACE

There is no doubt that land, sea, air and space are all physical domains. To put it simply, they exist and are natural. On the other hand, cyberspace is an artificial domain or virtual world created by human beings. Since our ultimate objective is to define “cyberweapon” we will concentrate on the word “cyber” which derives from the Greek. It means “to pilot or govern” or, in plain English, “to control”. Curious is the fact that today we are no longer in control of the present cyberspace because back in 1969 if scientists wanted to shutdown the network such would have been easy. Now it is truly impossible! Why? In 2019, humans have attached many aspects of their lives to cyberspace making Internet the dominant platform for life. Just think of the numerous things you do daily that require an online connection and in the nearby future with the Internet of Things (IoT) everything (people, mobiles, cars, houses, etc) will be fully interconnected [2].

What is Internet after all? Undoubtedly a great paradox because even though it is regarded as a virtual world, it nevertheless consists of a multitude of physical objects like computers, modems, networks, routers, servers, cables, printers, smartphones, satellites, etc. For example, if I only have a desktop and just use it to write a book then my computer is not online. Yet, if I buy a modem and link it to my desktop then my computer becomes part of the well-known public Internet. At this point, it is very important to acknowledge what is an intranet and extranet. The first is the internal network of a company or a private Internet because only the respective employees have access to the given intranet. The latter is something exterior to the given company but still associated with that company. For example, clients and suppliers use an extranet or external network to access the database of the company. It should be obvious that their access is restricted so the database itself and the data contained in it are not at risk. What matters is that both intranet and extranet make use of cyberspace.

How to explain what cyberspace is? The best way is to compare it with physical space. Consider a private home with a garage large enough to fit 100 laptops. If the family connects all these computers with cables then they have established a local-area network (LAN) via Ethernet. Now, the computers can communicate with each other. Note that these laptops are not online but cyberspace is present. The same holds if the LAN is erect via Wi-Fi or Bluetooth because in these two cases, cyberspace represents the wireless communication link existing among the laptops. Suppose that the family decides to connect this LAN to the router that is located in the kitchen. If they do so, then the local-area network connects to Internet via cyberspace and all 100 laptops are online. To summarize, cyberspace is the resulting virtual space from any technology that is able to connect two or more devices.

Not surprisingly, such notions have spilled over to the military realm. Given the four traditional spheres (land, sea, air and space), cyberspace is the fifth and vital domain. Three reasons are information, speed and communication. Thus, a party that achieves full control of these three parameters is bound to be a winner in any conflict. In other words, whoever controls cyberspace is in command of the military operations. It should be clear that this is the main threat of our prevailing scenario. For example, in a recent past, the machine-man systems controlling the firing of nuclear weapons had no connection to cyberspace [3]. Many factors including lack of confidence on the human element resulted in the modernization of the respective systems that inevitably brought inside the loop information and communications technology. The logical drawback is that under such conditions a hacker that gains access to the system may either neutralize the nuclear weapon or fire it at the target he wishes. Further, since the infrastructure behind Internet is both public and private certain countries are trying to build their own Internet. If they succeed then these virtual networks would be entirely controlled by the leaders of those governments.

5. JUMP FROM VIRTUAL TO REAL

Note that as technology advanced our characterization of weapon become more ample and deadly. At first, it was a physical object (solid and non-organic) then it became multi-state (gas) and changed form (organic) like chemical and biological weapons, respectively. Another pattern is that as the entity became smaller its destructive power increased by many orders of magnitude. Unfortunately, a nuclear weapon is the perfect example since it splits the atom itself. Thus, we started with standard weapons and finished with weapons of mass destruction. The only common denominator is the fact that these pertain to the real world. How does cyber and cyberspace fit into this trend if there is any at all? Fifty years ago, we could have never imagined the power of the Internet. Today, we know! The interconnection of all military branches via cyberspace created a gap between the virtual and the real but the menace is the possibility of jumping such gap. It should be plausible by now to think that the only entity that can jump from virtual to real is a cyberweapon and not a cyber-weapon.

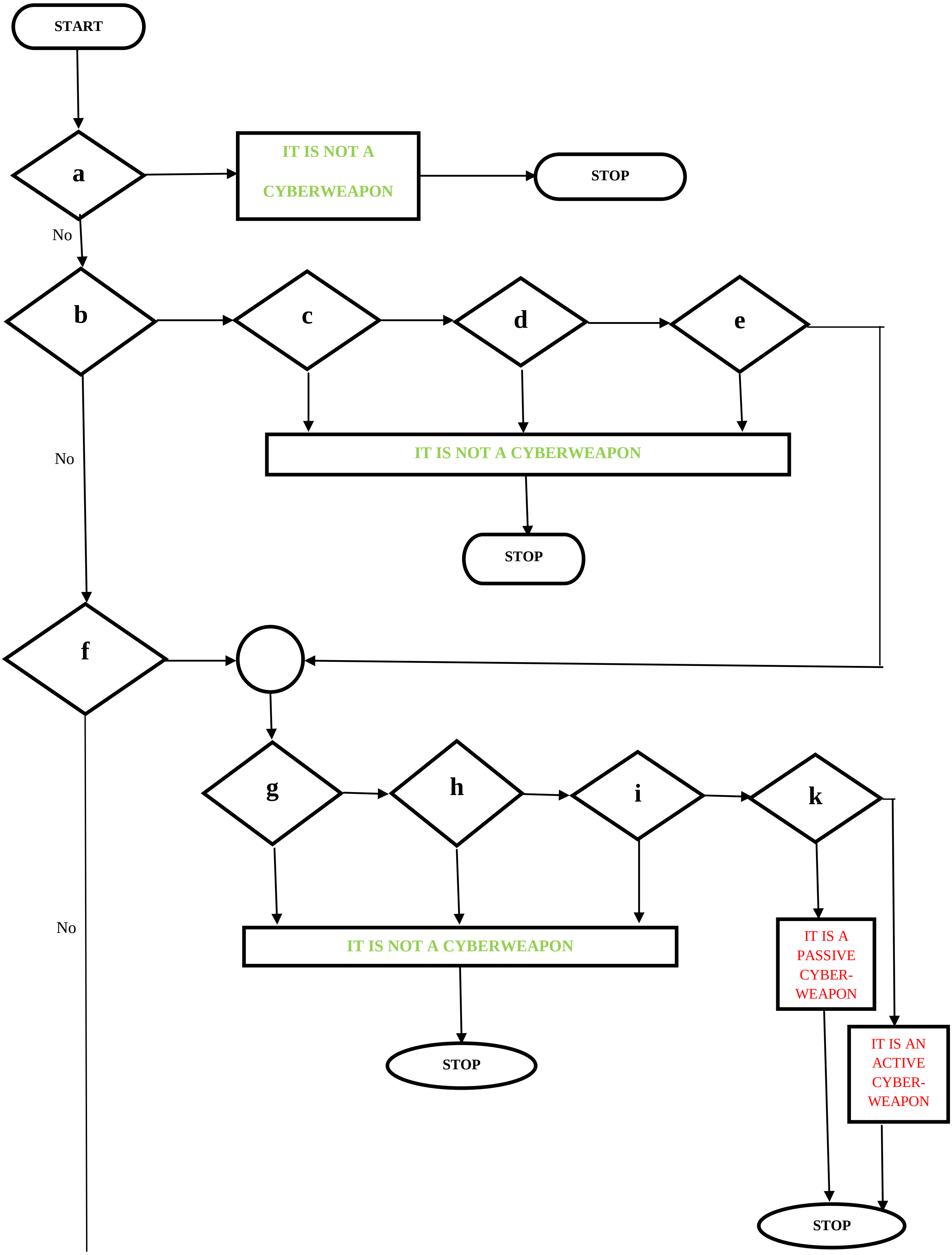
Why must we join the words "cyber" and "weapon"? Ponder the following real-life situation. Atomic bombs have been detonated underground, in mid-air and underwater. This means that the surroundings mediums were solid, gas and liquid, respectively. In all three cases, an explosion took place. Thus in the real world the medium is not intrinsically connected to the weapon. If a submarine fires at a warship – the torpedo travels thru water – before it strikes the given ship but the ammunition is not called "watersubmarine" nor "watertorpedo". Now think about cyberspace or even the word itself. Such artificial space only exists in the cyber domain. Disconnect all the devices (cables, router and computers) and the local cyberspace vanishes. For example, when I send an email what I am actually doing is electronically transmitting information to another computer. As a result, the word "**email**" is a fusion between "**e**lectronic" and "**mail**". In addition, consider the term "cyberattack" and its 2010 definition by the Committee on National Security Systems of the USA:

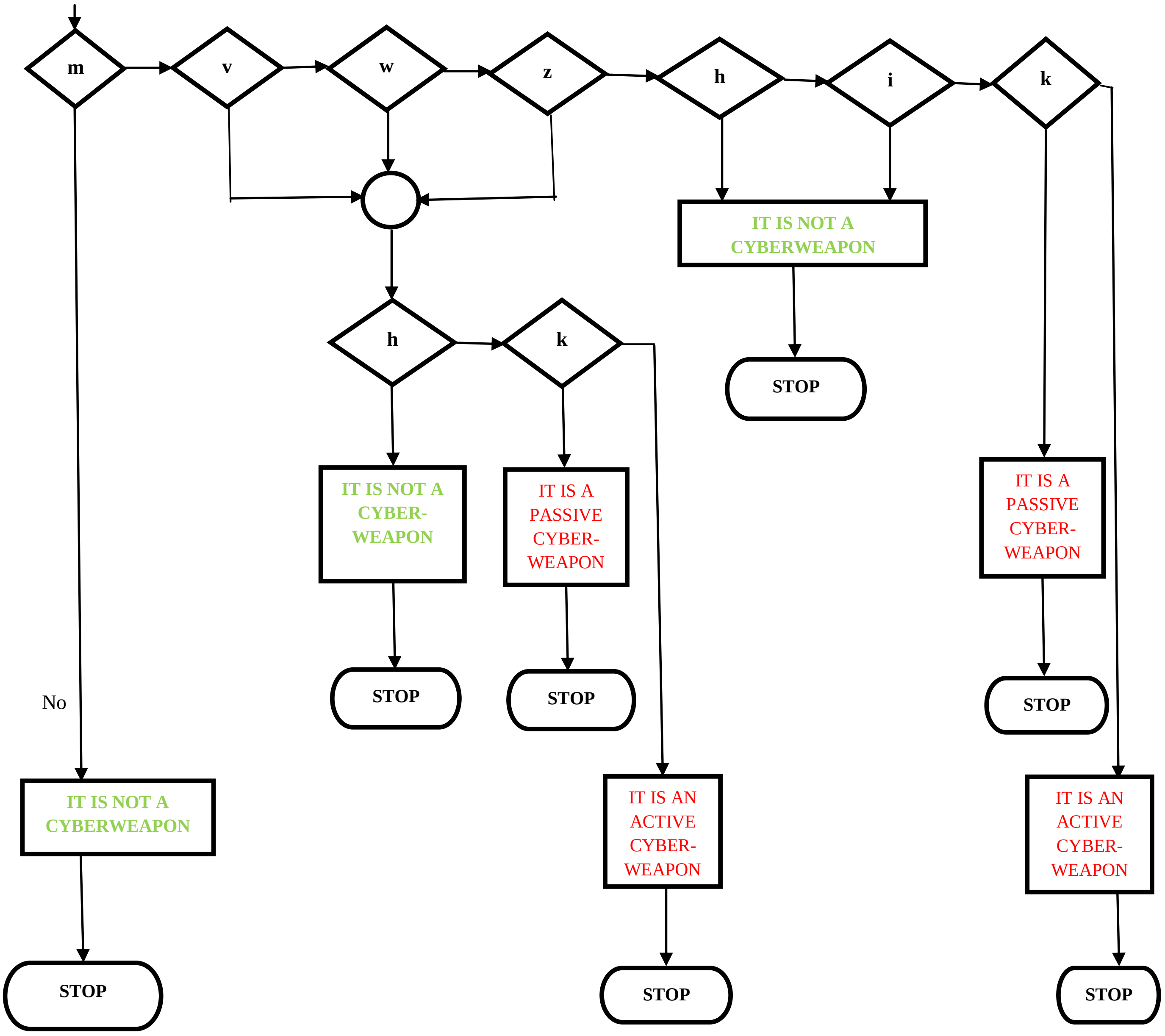
“Any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself”[4]. Accordingly, there are two types of attack (passive and active) and either one must occur via cyberspace. Assume the following fictional scenarios. I am online and without thinking open an email with a link that contains malicious code (software keylogger) and start typing my password on the keyboard to check my email. The next day, I am unable to enter into my email account. Such is typical of a passive cyberattack where personal information has been collected. On the other hand, suppose that I have an ecommerce site and my old clients complain that they cannot access it. The reason is because I was a victim of an active cyberattack known as denial-of-service (DoS) where system resources are no longer available. Nevertheless, it should be clear that in both types of attack the medium (if we may call it as such) is cyberspace. This is the argument why we must join “cyber” with “weapon” to obtain cyberweapon.

6. CYBERWEAPON AND ALGORITHM

A trend exists because the creation of cyberspace caused a unique transition from the concrete to the intangible. In the real world, things consist of matter while in cyberspace everything is in terms of bits. Every bit has two states like ON or OFF corresponding to 1 and 0, respectively. For example, the integer 5 is equivalent to 101 in binary notation. In fact, it is possible to represent almost anything (computer programs, images, sound, etc) as a sequence of binary digits. Engineers work with two kinds (continuous and discrete) of signals. An example of a continuous signal is the corresponding voltage from any electrical outlet of your house depending where you live. The running clock of any digital computer is an example of a discrete signal. Also, three pillars of information and communication technology are data, information and knowledge. Data can be anything from numbers to letters; you name it. Information can be the following: “A prime number is only divisible by one and itself”. The last level is knowledge such as “The distribution of prime numbers hidden within a fractal binary pattern” [5]. Have you ever heard the phrase “Knowledge is power”? [6]. Well, the transition previously mentioned concerns the realization that today, information alone is also power. A vivid example is the weaponization of social media where letters that someone types on their keyboard become words in some digital platform and these eventually result in the killing of people somewhere in the real world [7]. Thus, this is the trend. It is becoming easier to harm another human being in both cyberspace and the real world. Hence, what is a cyberweapon? Whatever it is, it must be able to jump from the virtual world into the real world and must have the potential to kill and/or destroy. A striking example is the Aurora Generator Test conducted by the Idaho National Laboratory (USA) in 2007. The basic idea was to show that the electric power grid could be vulnerable to a cyberattack [8]. We will concentrate our attention on the system (physical and logical) surrounding the given generator. First, a large diesel engine drives the generator. Second, we assume that the system has minimal security. Third, the entire system is isolated from the public Internet. A few key parameters (frequency, voltage, etc) must be synchronized in order to connect any source to the grid. In fact, the Aurora attack consists in sending via remote electronic access a series of commands to the control systems behind the generator. The goal is to cause a circuit breaker to rapidly open and close out of synchronism. As observed in 2007, the resulting mechanical and electrical stress made both the engine and the generator shake to the point that pieces of the coupling were ejected far away. Such pieces are like bullets so if someone was nearby they could have been hurt or even killed. After a few minutes of malicious operation, the generator was critically damaged and the test was completed.

In pages 9 -10, I present an original algorithm whereby given any input, the user can know if the input is or is not a cyberweapon. In fact, there are two types of cyberweapons: passive and active. Eventually, three are the outputs. One, it is not a cyberweapon. Two, it is a passive cyberweapon. Three, it is an active cyberweapon.


START
a
IT IS NOT A
CYBERWEAPON
STOP
No
b
c
d
e
IT IS NOT A CYBERWEAPON
No
STOP
f
g
h
i
k
No
IT IS NOT A CYBERWEAPON
IT IS A
PASSIVE
CYBER-
WEAPON
STOP
IT IS AN
ACTIVE
CYBER-
WEAPON
STOP


m
v
w
z
h
i
k
IT IS NOT A CYBERWEAPON
STOP
h
k
IT IS NOT A CYBER-WEAPON
IT IS A PASSIVE CYBER-WEAPON
STOP
STOP
IT IS A PASSIVE CYBER-WEAPON
STOP
No
IT IS NOT A CYBERWEAPON
STOP
IT IS AN ACTIVE CYBER-WEAPON
STOP
IT IS AN ACTIVE CYBER-WEAPON
STOP

a = IS IT A POLITICAL OR PHILOSOPHICAL IDEA? **b** = IS IT A MATHEMATICAL IDEA?

c = DOES SUCH IDEA SOLVE ANY OF THE MATHEMATICAL PROBLEMS IN CRYPTOGRAPHY?

d = IS THIS SOLUTION ACCEPTED BY BOTH ACADEMIA AND INDUSTRY?

e = CAN IT BE IMPLEMENTED AS AN ALGORITHM?

f = IS IT AN ALGORITHM? **g** = DOES IT RUN IN POLYNOMIAL TIME OR FASTER?

h = DOES IT HAVE THE POTENTIAL TO KILL AND/OR DESTROY?

i = IS THERE A PROOF-OF-CONCEPT? **k** = IS IT ONLINE? **m** = IS IT A COMPUTER CODE?

v = IS IT A VULNERABILITY? **w** = IS IT A CRITICAL VULNERABILITY?

z = IS IT A ZERO-DAY?

7. THREE CLASSES OF CYBERWEAPONS

Many boxes of the previous flowchart only contain single bold letters. Due to paper limitations, the size of those boxes was too small to write the full description of the respective box. From here on, we designate a single bold letter as Part and several bold letters as Path. For example, Part **a** represents the question: Is it a political or philosophical idea? Likewise, Path **b-c-d** concerns three mathematical related questions. At this stage, we are ready to introduce the different classes of cyberweapons: possible, known and unknown.

The first class is a possible cyberweapon described by Path **f-g-h-i-k** or a polynomial algorithm. An example is finding a fast way to factor large composite numbers. Part **h** represents the question: Does it have the potential to kill and/or destroy? Recall that our first definition of weapon was associated with a physical object. Cyberweapons are more subtle. Now, destroy may also signify the collapse of an industry, of the social and political order, etc. Hence, the answer is yes since finding an efficient method to perform integer factorization would render RSA cryptography obsolete causing a great turmoil at the economical level. Part **i** pertains to a proof-of-concept (PoC) or the verification that some idea is feasible in the practical sense. In theory, all you would need to do is apply your algorithm to a large semiprime like RSA-1024 bits and show that it can find a prime factor in a short span of time. Part **k** questions if this algorithm is online or offline. Hence, if such information is online then we have an active cyberweapon because the algorithm is of public domain and anyone can do anything. Here the adjective “active” is completely different (in meaning) from that of an active cyberattack. Active signifies that the given cyberweapon is available in cyberspace, consequently, there is the constant threat that it may achieve its objectives whatever they may be. On the other hand, if such information is offline, we have a passive cyberweapon. Why? Suppose the following plot. Someone discovers an ingenious method to factor numbers and does not tell anyone. In addition, this individual confirms that such technique works since he/she is able to factor

RSA-2048 bits in one week using a single computer. Once again, here the adjective "passive" is different (in meaning) from that of a passive cyberattack. Passive signifies that this cyberweapon is a potential danger for given the fact that someone found a fast solution such implies that it exists and therefore another person may think the same.

The second class is a known cyberweapon given by Path **m-v-w-z-h-i-k** or a malicious computer code. A clear example is Stuxnet considered by most experts to be the first-ever cyberweapon [9]. Such worm was able to destroy and damage many centrifuges (electromechanical devices for separating nuclear material) at an Iranian nuclear installation. It was discovered around 2010 and the complexity of its code is amazing. In cybersecurity, there are three basic levels: vulnerability, critical vulnerability and zero-day. Stuxnet contained four zero-day flaws among other malicious code. Part **k** questions if it is online. It is evident that Stuxnet was online but here we consider both alternatives. If such knowledge remained closed in some safe (offline) it would still be a passive cyberweapon or potential danger. Once shown that it is feasible and works, others may eventually do the same.

The third class is an unknown cyberweapon given by Path **m-v-h-k** or something that has not occurred yet. It is a computer code but it contains no computer-software vulnerability. If you permit my imagination to run wild. Suppose someone writes a book and transforms it into an ebook in PDF (Portable Document Format) thus creating a non-malicious electronic file. Contemplate that the entire contents of this ebook tries to answer the most fundamental questions of human nature. Assume that the given PDF is freely available online and people start to download it. Next, they read this "new bible" and begin to believe in it but fervently. At this point, the world is divided between two bibles (old and new) and violent clashes take place at a global scale. The outcome is a great bloodshed and massive destruction of private property. There is no doubt that such scenario is far-fetched but it is not utterly impossible.

8. TESTING OUR ALGORITHM

Now, that we have an algorithm the most logical step would be to test it. But test it with what? Today, we know about Stuxnet so it is easy to verify with our flowchart that such is an active cyberweappon. Yet, the situation is very awkward with respect to any future cyberweapon. Two are the cases that we must consider in detail. As a passive cyberweapon is offline and if the other party is unable to get hold of any information concerning it then they are unaware of its existence so the menace is only potential. In the case of an active cyberweapon, various scenarios can take place since it is online. First, the cyberweapon fails to work. Second, its impact is minimal. Third, it functions as designed. Please note that in all three circumstances both parties (attacker and defender) must obtain subsequent information (direct or indirect) following the deployment of the given cyberweapon, otherwise, any assessment of it is impossible.

Cybersecurity is a relatively new field that consists of many different disciplines. As a result, many terms such as cyberwar and cyberpeace still await a formal definition [10]. Establishing a valid terminology as soon as possible is of crucial importance in order to resolve issues like which malicious deeds in cyberspace should be considered as acts of war? In this respect, the present algorithm (flowchart) is the first method that is capable of distinguishing a cyberweapon from any weapon. Thus, anyone or any nation that is engaged in advanced research can use the previous flowchart to check if what they are actually doing (design, code, build and test) is indeed a cyberweapon. At first glance, this may seem contradictory (how can it be that a scientist or a group of researchers are not aware of their actions?) but two simple facts will provide a fair explanation. First, many were the times that scientists intensely searched for a very specific entity and ended up finding something entirely diverse on the way. Second, when the Internet was in the making, everybody had a clear idea regarding the final objective of the project. Today, many researchers realize that Internet is the first thing that humanity has built that humanity does not fully understand.

9. CONCLUSIONS

In this work, I tried to define the term “cyberweapon” and presented my arguments for why I write it as such. We started by analyzing the words “weapon” and “cyber” which took us from the real (land, sea, air and space) to the virtual (cyberspace). At this stage, we found ourselves in uncharted waters. The possibilities emerging from this new domain seem infinite. In fact, Internet has profoundly changed the world for better and for worst.

Unlike standard weapons which are easily identifiable by their tangible form, the notion behind a cyberweapon can be very vague both in essence and substance. Fortunately, our research established some basic ground and as a result, we created an algorithm to identify both the type and class of a cyberweapon. Thus, there are two types: passive and active. There are three different classes: possible, known and unknown. Note that I am fully aware that reality (present or future) may contradict these findings but my main objective was to set up a solid starting point for further study. From a technical view, a cyberweapon is a digital entity that uses cyberspace to jump from the virtual into the real and, in doing so, destroys and/or kills. Stuxnet is the prime example. But since its first appearance around 2010 we can be sure that it is not the only cyberweapon. Where are the others? Who controls them? These and other relevant questions pertain to the global arena of politics and diplomacy or, shall I say, cyberpolitics and cyberdiplomacy. Nobody knows what lies ahead but one thing is certain. As our technology evolved so has its power of destruction. Cyberwarfare may not be the last frontier. Yet, free available knowledge and cyberspace makes each one of us both a target and a cyberwarrior. I sincerely hope that whoever or whatever makes the final call with respect to any future cyber conflict never forgets the ultimate difference between machine and human being. While a machine has no history of its own, we have survived natural global disasters including self-destruction. Furthermore, for some reason, human beings are still the sole creators of every single machine existing on this planet and beyond.

REFERENCES

[1] S. Mele, *Cyber-weapons: legal and strategic aspects*, Machiavelli Editions, June 2013, Available from https://www.strategicstudies.it

[2] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: what everyone needs to know*, Oxford University Press, New York, 2014.

[3] A. Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, Georgetown University Press, Washington, DC, 2018.

[4] D. S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Georgetown University Press, Washington, DC, 2012.

15 [5] J. C. L. da Silva, *The Rainbow of Primes*, Freund Publishing House, Tel-Aviv, 2009, 63-84.

[6] L. Floridi, *The Logic of Information*, Oxford University Press, Oxford, 2019.

[7] P. W. Singer and E. T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Hartcourt Publishing Company, New York, 2019.

[8] M. Zeller, *Common Questions and Answers Addressing the Aurora Vulnerability*, DistribuTECH Conference, California, February, 2011.

[9] N. Falliere, L. O. Murchu and E. Chien, *W32.Stuxnet Dossier*, Symantec Security Response, November 2010, 1-63.

[10] M. Christen and E. Bangerter, *Is cyberpeace possible?*, Zurich Open Repository and Archive, Zurich, 2017, 243-263.