RETHINKING CYBERSECURITY : A QUICK TRANSFORMATION

Nezir AKYEŞİLMEN[*]

Cybersecurity has been a popular concept and widely used in media and academy in recent years. It has both technological and social dimensions. It is so important that should not be left to the technicians alone. The individuals, politicians and decision-makers need to deal with it and take proper measures. Cyber failure is not only technical but much more political. Therefore, we need policies that aim to provide a safe cyberspace.

Transformation of International Conflict Trends

Even though there is no general consensus on the definition of conflict, it is widely accepted that the idea involves a wide range of things ranging from a simple ideas conflicts to wars. In this framework, conflicts can be classified into different forms. For instance, in a broad sense, violent and non-violent conflicts; or they can be examined in five categories: first two groups are latent/hidden (disputes) conflicts and manifest/conflicts (non-violent crisis). There is no physical violence in these two conflicts. The third group is crisis or violent crises. The fourth and fifth are limited wars (severe crisis) and wars. Another classification can be in the form of interstate and intra-state conflicts.

The trend of world conflicts changes from time to time according to technological, economic, cultural and political development at the global level. In general, the number of violent and non-violent conflicts in the world is close to each other. But from time to time this number has increased in favor of one. Especially during the post-Cold War period, the number of conflicts has declined in general (the number has fallen below 100 in the whole world in 1990s), especially in interstate conflicts. As of today, 189 of the 409 conflicts that exist in the world are non-violent, while 223 are violent ones. Of these, 180 are violent crises, i.e violent rarely appears. Only 71 of these conflicts are among the states, while 338 are within the states. 42 of them have intense violence that can be accepted as wars (both limited and full wars). And most importantly, none of these take place between the states. And yet none of the 42 conflicts occurs in democratic countries. All intense violent conflicts occur in non-democratic or semi-democratic countries. Only 10 out of 180 violent crises are among the states.

[*] Assoc. Prof. Dr., Department of International Relations, Selçuk University, Konya-Ankara. Can be accessed via nezmen@yaho.com

In summary, the trend of conflicts in the world is as follows. The number of conflicts is increasing. In the last 20 years the number has increased fourfold. Conflicts are increasingly being drawn into the state. More than 80% of the conflicts in the world are in the state. There is little or no violence in the conflicts between states. Likewise, in democratic countries conflicts either never exist or do not involve violence. In other words, democracy is a system with the ability to solve social and political conflicts without violence.

In recent years it has also been mentioned about cyber conflicts. This new type of conflict will affect the world's conflict trend. Before gong details, I would like to focus on the concept of "Cyber war", which is discussed extensively in the cyber policy literature. Some analysts both on the cyber-technical side and on the political side use this concept in an unreasonable and unnecessary way. If conflict management and international legal literature are taken into consideration, the concept of “cyber war” seems to be meaningless and unnecessary today. Why? Because, war is the most violent type of conflict that also contains high physical damages. However, there has not been any cyber attack from that have been made up to now, except for the Stuxnet (limited range), which causes physical damages. First of all, the concept of "cyber warfare" is a harmful concept that serves a security mindset that helps to securitize the cyberspace. It is a usage that gives the greatest damage to human rights and freedoms of the individuals. It is not innocent or ignorant. Then why do some people like to use the concept of "Cyber warfare"?

One reason is the effort to show that the area very important. Cyber space is already important, people feel it in their daily life. But they only damage the area by securitizing it. The second is to attract attention. The third is intended to serve relief, that is, securitization and ultimately from ignorance. Since, in international law and conflict management disciplines, such conflicts can not be defined as war on any criteria. If the nature of these attacks changes tomorrow, they can be accepted in the war category, but today there is no such conditions.

Technically cyber attacks are also cyber conflicts. Cyber conflicts are usually continuation of a kinetic conflict. There are too many types of cyber conflicts. But the ones that can be considered as cyber political conflicts are numerous. They are also quite effective on global politics and security policies. Unfortunately, globally, cyber conflicts have not been shown in world conflict maps or barometers yet. But they will be taken into consideration in the near future. Cyber conflicts will affect the world's conflict trend in a significant way. As can be seen in the statistics given above, the number of violent conflicts between states is very small in the world. This is quite understandable, as states are avoiding it because a conflict involving interstate violence has a great deal of destructive power. I mean, there is some kind of deterrence in that sense. But since cyber conflicts do not involve physical violence as of today, the likelihood of such conflicts increasing at an international level is very high. The simplest example of cyber attacks alleged today for the US elections continued between the US and Russia. Similarly, cyber intelligence tensions between China and the US is on the agenda. Since these conflicts do not involve violence, as between states and non-state actors, the number of such conflicts will increase from day to day and unfortunately will often trigger other conflicts involving physical violence.

The world is heading towards a hybrid conflicts that have cyber and physical dimensions. Cyber conflicts are increasingly affecting our lives and continue to grow at a pace that will also impact international conflict and security trends.

Towards a Global Cybersecurity Question

Considering the effects of cyber conflicts on humanity, the concept of cybersecurity has become an important component of national and international security, targeting the infrastructures that have reached a rather deadly and destructive stage in recent years, not only individuals or private companies, but also social service sectors. A code can create a global chaos. How vulnerable is an environment such a fragile system? With a simple software program, planes can be prevented to fly. Digital machines can be controlled or taken out of control. Can not this all be a doomsday for people?

The concept of cyber security has become a very popular concept in recent years due to the hacking of big companies like Yahoo, BBC, Paypall, Amazon and recent discussions on US elections. Even though it was an important issue, people could not realize it before they were exposed to the cyber attack, and they regarded it as insignificant. But now, cyber security has become an important security question that includes national and international security beyond just a secure cyberspace. 2007 Estonia, 2008 Georgia, 2010 Stuxnet virus and 2011 Israeli attack on Syria are the clearest examples of this.

What is the cybersecurity? Is a full cybersecurity possible?

Everyone uses the concept of cybersecurity in different meaning and for different purposes. There is no globally accepted definition on the world, as there is no agreed agreement on this issue. The National Cyber Security Strategy and Action Plans of each country make different definitions. Naturally different definitions force each to take different measures, even though some are similar.

The problem is not just that everyone has different definitions. The problem is that no one question this concept. Everyone receives the concept of security of cyberspace as a given concept and accepts their definition as the most accurate one. But no one asks the question of who security? What types of security? and how to manage it? These are the questions that should be asked in national strategy action plans. In addition, academic studies continue with the same infertility.

The national action plans and literature heavily focus on the information and network security. However, the user is the most important component of cyberspace. Unfortunately, in the literature, the user in that sense, is generally ignored. While discussing the IP / TCP layers of the Internet the use, is constantly being emphasized as the most important layer or component of the internet, yet this element is kept out of sight in security debates.

For this reason, the vital question is the security for whom? If we proceed in this direction, a more healthy definition and series of measures can be developed. The measures that can be accepted by all cyberspace stakeholders. The stakeholders of cyber space are people, private companies and states. But today’s global system, states alone can make decisions on behalf of other stakeholders. For this reason, they can not fully implement the decisions they make. Why? Because, unlike physical spaces, the dominant actors of cyberspace are not the states anymore. I.e. the cyberspace is not a state-centric environment. For this reason, if cyber is to be secured in the world, the states will not act on their own but will act jointly with other stakeholders. Such a strategy, taken into consideration all stakeholders' demands and requests, can only provide cybersecurity. In the world of cyberspace, national security is not possible without ensuring the safety and freedom of the individual. To shot down internet is not a cybersecurity measure. It's an indication of inadequacy. This is usually done by third world countries where the cyber Know-How is too weak or does not exit.

The main objective of cybersecurity is confidentiality, Integrity and accessibility (CIA) of information. The interruption of access means that there is no cybersecurity. Security, accessibility and privacy are at the same time human rights and freedoms. No cybersecurity measure that does not target the protection of human rights and freedoms can provide real security. Just like in real life.

Evolution of Cybersecurity

The digital world or cyberspace with its most common name, continues to influence our daily life. Alongside the benefits and opportunities it has provided in recent years for the individual, institutional, national and global actors, it has brought threats and weaknesses, especially in security sector.

More than half of the world's population, 3.8 billion people use the internet today. Worldwide, the number of websites hits 1.3 billion today, despite the first was opened in 1991. More than 200 billion e-mails are sent on average per day. Again, five million smartphones are sold per day (source: internetlivestats.com). 1.2 billion machines are connected to the internet today and it is expected to reach 10 billion by 2020. Online trade volume has exceeded 10 trillion dollars. Smart houses, intelligent cars, intelligent home tools and devices, intelligent machines and robots are the benefits that facilitate, accelerate, and comfort people's lives.

But it should not be forgotten that every vehicle connected to the Internet creates a security vulnerability. Because everything is increasingly connected to the internet, and as a result everything becomes available for hacking. The number of daily malware or daily viruses in the world is over 500. The number of attacks is expressed in millions. An average of 50 thousand websites is hacked every day. These are pretty big and scary figures.

Cyber attacks can also adversely affect or prevent public services (attacks on critical infrastructures) and private services (especially attacks on finance and energy infrastructures), that also threaten the confidentiality, integrity and accessibility of information. In recent years, cybersecurity has become increasingly a national and global security problem. Cybersecurity has gradually become a global security issue today.

In the early days, cyberspace was seen as a low politics area such as entertainment, economy and communication, but in recent years this area has been seen by states as a high politics area such as security, strategy and military. One of the most important questions in cybersecurity as stressed above is whose security? Although the answer to this question has changed over time, it still has not found a healthy answer today.

The Internet was built on information sharing and transparency from 1969 until 1988 (the first virus appeared in 1982 though was not used in an attack that would cause harm). But in 1988, when Morris worm was produced and left on the Internet, it damaged thousands of computers in the United States. For this reason, cybersecurity in the 1990s was perceived more as a problem of personal information security. Then, in 2000, a 15-year-old student made DDoS attacks on global corporations such as CNN, Yahoo, e-Bay, and Amazon, destroying them and damaging billions of dollars after which, cybersecurity has become an important corporate security issue for private companies. However, in 2007, DDoS attacks on Estoya, Israel's control of the Syrian radar system, Russia's resorting to cyber attacks with physical attacks in Georgia in 2008, and finally, as the first cyber weapon the Stuxnet, produced for attacking Iran's nuclear facilities, the state has then begun to perceive cybersecurity as a national and international security problem.

Today, cybersecurity has become a crutial component of global security. For this reason, countries have been publishing National Cyber Security Strategy Documents in recent years and are making huge investments in cybersecurity. Defence units are set up in the face of cyber armies and cyber attacks (made up of hackers).

In the last National Security Strategy document of the United States, cyber space has been considered under the heading of international security and is described as a major threat. The document, which emphasizes that cyber conflicts have become an important issue of international security, mentioning of measures to be taken in for this purpose.

To sum up, cyber space, seen as a world of opportunities, has now become a space that also contains significant threats. This area, which generates security issues from the individual level to the global level, is also an important power tool at the same time. For this reason, nobody can give up on it. The most important measure for safe use of cyber space is personal consciousness and national cyber policies. Because the weakest link of cyber security is the user, the individual. Again, cyber security failure is far more political than being technical. That is, lack of appropriate and applicable policies. Perhaps the most important and crucial point is that cybersecurity can only guaranteed via morality or ethics. Just as morality is in the physical world, in the cyber world it is also the most important indicator and guardian of our humanity.

In short, cybersecurity is a relatively new issue, but has been very popular concept and effective at the global level. In order to catch up with social, economic and political measures need to be taken along side with the technical and technological improvements. Policies are as important as technological innovations.