International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 638-640 www.ijaem.net ISSN: 2395-5252

Cyber Space and Cyber Security Question

Amol Hankare

Date of Submission: 15-07-2023 Date of Acceptance: 25-07-2023

After the end of Cold War, World has globalized rapidly and digitalization process developed with globalization. Technological improvements mostly focused on development of military capacity during Cold War. However, when fall of Berlin Wall and dissolution of Soviets Union, ideological confrontations finished and world has adapted neoliberal globalization politics of West which leading by US. Discovery of internet and dissemination of its usage has the leading factor of digitalization process of world. Spread of usage of internet became uncontrollable. In international relations, system rely on state’s behaviours and state’s rules. System elements generally established by states and its control and direction mostly hand of nation states. However, we have to note that, usage of internet and development process of technology happened rapidly in scientific studies. States have not controlled that improvement. This uncontrollable development of digital world also brings in its wake weaknesses of that department for states and private sectors. This process has accelerated in first years of twenty first century. States realized that development of digitalization became one of national security issues and it caused notably economical questions in last years. Cyberspace concept has become important definition of new digital world, which is physical and virtual area, rely on stocking information in digital world. This information includes states private information’s as secret military information, collecting taxes, election process etc. At the same time, digital world indispensable area for private sector business as relations with companies, monetary calculations etc. Technology has become the most prominent elements of international system in the world today.

As I mentioned above, development of technology and its usage in daily life has separated rapidly in last thirty years. That has provided many advantages for human life in any sector. However, it also caused weaknesses of protecting information as private information. Cyber security emerged from these weaknesses of preservation of knowledge and information. That question increases rapidly for the entire world. Internet usage continued to increase and its expansion has reached a huge number. In the world, while several people could not connect internet, more than 3 billion people have connection in internet in the world. Digitalization of the world and usage of internet also has helped globalization of the world. Creating of global village concept may be possible with expansion of usage of internet. Briefly, global village means, any local issue has potential became global issue in the world. Especially in last years, globalization of local problems has more effects in international relations. Social interaction in internet with Twitter and Facebook’s effect to gather people in certain areas during Arab Uprising protests in Middle East.

However, Economical losses and preservation of secret information which belong to states are the most prominent question of cyberspace for international society. According to the studies of Rand Corporation –which is think tank association in US-, there is almost 345 billion $ loses in a year because of cyber-attacks in the world. In addition, states and private companies has invested 70 billion $ for cyber security in a year in the world. That may show us the importance of cyber security question for the international society. That statistics also show us, states has realized its vulnerabilities against cyber-attacks to national associations and private sector. Although awareness of vulnerabilities by states, there is no still effective response methods to threats in cyber space. Absence of effective coordination between states also caused harder situation in order to fight against cyber criminals. Only developed and some developing states has taken some measures against cyber threats. That obstruct fighting against cyber-attacks as international level. However, there is a significant question in that point. Do states really want to fight against cyber threat or they try to use it for taking advantage against other states? I think, that is the prominent question for cyber security issue.

Although there is no still effective coordination between states in order to struggle against threats from cyber space, there has some efforts to take control of cyber space with the hands of nation states. World Summit on Information Society was began to efforts about cyber security on the state level which organized by United Nations. The WSIS intergovernmental initiative is a milestone in its own right as it sought to combine several distinct aspects of the UN's twentieth century development agenda with emergent implications of information technology. WSIS was the first comprehensive response to the emergent "virtual" global society in a world which increasingly concerned with the dilemmas of sustainable development. Although it was not conceived as a security centric activity, the WSIS objectives that dealt with cyber security were broadly consistent with developmental concerns. WSIS held in conference in Geneva and Tunis which rely on creating awareness of cyber security and building coordination between states. Almost all of UN's members has committed to WSIS's action plan in order to struggle with cybercrimes. Action plan was accepted by states, which is called "Action Line C5", but countries implementation of plan actively has debatable. Because, there is no still common definition of cyber-crime and how responsibilities of cyber-crimes punished in international law. Absence of judicial process of cyber-crimes also another important problem for cyber security issue. Absence of judicial process of cyber-crimes also prominent question for nation states. Rising of criminal activities in internet as global level in last years, pushed to states taking hard preventions against cyber-crimes. US is one of the leading countries that is taking firm preventions against violations of private information or goods in daily life. For example, a woman punished with hundreds of thousands of dollars due to downloading movies and music with torrent in recent years. On the other hand, mostly, following of illegal activities in internet could not catch by states' cyber investigation bureaus due to unprecedented structure of internet realm.

New institutions were created in order to fight with cyber threats, which were created by national authorities with international scope. However, it has not interstate structure, which is called Computer Emergency Response Teams (CERTs). These are sole institutions, which has global effectiveness against cyber threats. CERTs try to identify vulnerabilities and generating connections between security vendors, users of digital materials and private associations. By 2009, there were over 200 recognized CERTS, with widely different levels of organization, funding and expertise. The purposes of CERTs explained (as) three basic tasks; firstly, a decreasing of unaddressed vulnerabilities of private and national associations, secondly, developing understanding of cyber threats frequency and natures which need to detect dimensions of cyber-attacks and finally, providing strength cooperation between all of CERTs. We may focus activities of US and European Union in NATO and EUROPOL. NATO established Cooperative Cyber Defence Centre of Excellence (CCDCOE) in order to inform and training member states of NATO. It established after the cyber-attacks in Estonia in 2007 by Russian hackers. The preserving of secret military information and defence plans against Russian aggressions have been under threat by Russian hackers and NATO have taken several measures for that. Russian, Chinese, Iranian and North Korean hackers perceive a national threat for Western countries and US try to take preventions against them via NATO and cooperating with EUROPOL. In addition, European Union has taken some measures against cyber threats and they established European Network and Information Security Agency (ENISA) for that. ENISA mostly focuses on informing and training process for internet security, and it cooperating with territorial CERTs but it does not provide enough large-scale defence against regional cyber-attacks. In recent years, cyber-attacks to elections in US and European Countries by Russian hackers has perceived most prominent threat. Elections in US on December 2016 resulted surprisingly victory of Donald Trump who was the candidate of Conservatives. After the elections, democrats accused Russia about intervention deliberately to elections in US and, they claimed that Russian hackers who are supported by Russian Federation intervene to the elections for the favour of Trump. US courts started investigation after the assertions of democrats and investigation continue during these days. After the discussions of Russian intervention to US elections, European countries has taken several preventions against possible Russian intervention to their elections too in this year. Even, Netherlands did not use any technological machines during her elections. They used traditional methods as using of paper for voting.

In the context of national security issue, Stuxnet is well known attack which organized by US and Israel in order to stop enrichment process of uranium in Iran. Stuxnet may called cyber operation which organized by a state to another state. There is important question in that point; May actions of US and Israel with Stuxnet cyber operation against Iran called as violations of sovereignty of nation state? As I mentioned, there is absence of law procedure for that question. In addition, Iran never prove absolutely Stuxnet attacks to its nuclear program was the organization of US and Israel. At the same time, even if they proved that, there is no clear action process what Iran defend legally itself. That have to determine clearly by states with conventions as international level. In addition, it is problem for US what will happen if Russian intervention to US elections proved.

For private sector, the effectiveness of malicious software has an substantial question. Several companies and individuals lost its money because of cyber-attack which organized by unknown hackers. Especially, banks have under the high-level risks. Banks always face threats of capturing its customs information. All of people in the world is under threat about capturing of its identities by hackers. For example, ErcanFındıkoglu were in jail because of rubbing of 55 million $ from banks in Germany. He was extradited by Germany to US. That is the basic example for cyber-attacks to banks or money accounts of individuals by individual cyber attacker. There is huge market about cyber defence computer software. The market for virus has been estimated at 2 billion $. Microsoft, McAfee and Kaspersky is one of the leading factories for that market. They may provide effective protection against cyber threats but, also there is trustship problem for these companies. People, companies or states never deliver its information to these anti-virus companies without doubt. Recently, Kaspersky found guilty about sharing private information of its users to Russian authorities by US courts.

In conclusion, absolute securitization of digital world is impossible because of its unclear structure. States has taken important steps to control cyber space in recent years but these are still inadequate for securitization of internet or technological machines. Because, digital world did not establish by states unlike other pillars of international system. Initially, it created and developed by private sector. Thereafter, states have complicated situation in cyber space.

CYBER BULLYING IS A SPECIAL PHENOMENON IN/DURING OUR THE SOCIAL MEDIA TIMES: it’ special, because now is a 24-hours activity. Now, in our times, combined with the Social Media and a smart phone, all the time connected to internet, cyber bullying it’s a 24/7-criminal activity, sometime in the open, sometime anonymous. With a Social Media connection, verbal bullying and cyber bullying is like a shadow that never leaves you on a shiny, sunny day. Coming home from school and/or your place of work, your Facebook, Instagram or Tweeter account will be flooded with cruel, negative postings, and as well other Social Media avenue will reflect your peers positive or negative image opinion about you.

So many digital software programs, Photoshop, design and editing program, can enhance with images and sound any other past (verbal, written, in my times) single dimensional bullying. Ridicule is taken to a whole new level with Social Media. Bullying never stops in Social Media Times. And because is electronic and digital media, only 1 and 0, it will stay and live forever, in a server, somewhere, close or far from you, but accessible in a fraction of second