Page 496 - 508 **DOI:** *https://doij.org/10.10000/IJLMH.111335*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Cyber Security and Cyber War

KARTIKEYE JOSHI[1]

ABSTRACT

Dependence on laptop systems has had a transformative effect on human society. Cybernetics is now woven into the core features of without a doubt every essential institution, together with our oldest ones. War is one such business organization, and the virtual revolution's effect on it has been profound. The American army, which has no peer, is form of absolutely reliant on excessive-tech laptop systems. Given the Internet's ability for entire-spectrum surveillance and records disruption, the marshaling of laptop networks represents the subsequent stage of cyberwar. Indeed, it's miles upon us already. In Cybersecurity: What Everyone Needs to Know, said professionals Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics took place and provide a purpose of wherein it's far headed. They start with an evidence of what cyberspace is earlier than shifting directly to discussions of the way it may be exploited and why it's so hard to shield.

I. INTRODUCTION

With the arrival of trendy era and additional information of the intricacies of cyber safety, it isn't always very difficult to count on conditions that have been idea to exist only in generation fiction films. Situations, in which an enemy attacks a rustic's pc device controlling a primary dam inflicting a flood; or in which the enemy corrupts the pc software which controls the united States's fighter planes or drones, and consequently the tool fails and starts off evolved attacking warring parties and civilians indiscriminately, are slowly becoming fact in the shape of cyber struggle.

When we communicate of 'war', traditionally, it offers with the strength of mind of hostilities that contain arms and greater exactly consists of a try and bodily wound or kill enemy opponents. Conforming to the layman's records of struggle, cyber struggle is likewise a type of contest of force and probably even of hands. However, such attacks aren't often public, and the factor isn't commonly to wound or kill enemy infantrymen, but to interrupt assets. The preferred consequences of cyber assaults are within the important oblique, due to this what may want to generally be taken into consideration secondary effects are in reality of applicable

[1] Author is a student at Law College Dehradun, Faculty of Uttaranchal University, India.

 [ISSN 2581-5369]

importance. So actually, the destruction of belongings, produces suffering among civilians and probable moreover combatants as foreseeable secondary effect. Countries' developing dependence on laptop networks eventually has expanded their vulnerability to cyber war. [2]

The Notion of Cyber Warfare: What is Cyber Warfare?

Cyber war has been described through the use of government protection professional Richard A. Clarke, in his book Cyber War (May 2010), as "moves by using manner of way of a geographical region to penetrate every other States's computer systems or networks for the functions of causing damage or disruption." The Economist describes cyber war as "the 5th vicinity of warfare," or maybe greater honestly placed it could be described as warfare conducted in our on-line world through Computer Network Operations (CNO) as approach and strategies. The term "cyber battle" consists of elements: cyber or our on-line world and conflict. Cyberspace may be described as "the worldwide digital communication and statistics transfer infrastructure" and "'war' is generally understood as relating to the conduct of military hostilities in conditions of armed battle" There are three important strategies of cyber struggle: sabotage, virtual espionage (stealing facts from pc systems thru viruses) and assaults on electric power grids. The 1/three is in all likelihood maximum alarming.

II. CYBER WARFARE A NEW WEAPON

The motive why cyber struggle is becoming a vital weapon is that the developing dependence of present-day militaries "upon strong, properly timed flows of massive quantities of statistics" technique that any "disruption would possibly quick have a crippling impact on the potential to combat". Furthermore, cyber war at the entire entails an assault on a laptop machine the utilization of every different computer. This way that cyber warriors often act remotely and release the assault from in the territory in their private nation, thereby lowering, or even putting off, the chance of casualties to their very own forces. Moreover, cyber conflict may additionally moreover purpose catastrophic results: "Computer insects supply down army email systems; oil refineries and pipelines explode; air-web site traffic-control systems disintegrate; freight and metro trains derail; economic facts are scrambled; the electric grid is going down. Orbiting satellites spin out of control. Society fast breaks down as meals turns into scarce and coins runs out. [3]

[2] Bhat, T.H., Khan, A.A. "Cybercrimes, security and challenges". International Journal of Advanced Research in Computer and Communication Engineering, Vol.6 (5) (2015)
[3] Arunesh Sinha, Thanh H. Nguyen, Debarun Kar, Matthew Brown, Milind Tambe, Albert Xin Jiang; "From physical security to cyber security" Journal of Cybersecurity, Vol. 1, Issue 1, 1 September 2015, Pages 19– 35.

 [ISSN 2581-5369]

III. INCIDENTS OF CYBER WARFARE AROUND THE WORLD

Cyber battle has been round as early as 1982. At the height of the bloodless conflict, in June 1982, an American early-caution satellite for pc detected a big blast in Siberia.

Computer code stolen from a Canadian business enterprise with the useful resource of Soviet spies brought on a Soviet gas pipeline to explode. The code had been changed with the useful resource of the CIA to encompass a logic bomb which modified the pump speeds to cause the explosion. This turned into one of the earliest times of cyber battle.

With the tap of a button and a few speedy keystrokes, cyber warriors can motive grave damages.

In 1991, it become recommended through air pressure that a laptop virus named AF/ninety-one become created and turned into established on a printer chip and made its way to Iraq through Amman, Jordan. Its pastime grows to be to make the Iraqi anti-plane guns malfunction.

The period amongst 1998-2000 witnessed the well-known assault named 'Moonlight Maze'. Moonlight Maze refers to an incident in which U.S. Officers via manner of danger located a sample of probing of computer structures at the Pentagon, NASA, Energy Department, non-public universities, and research labs that had started out in March 1998 and have been taking area for nearly two years. Sources said that the invaders were systematically marauding via tens of masses of files — which includes maps of navy installations, troop configurations and military hardware designs.

Cyber warfare calls for massive attempt to company, which even very advanced global locations are willing to place so as to extract vital facts from specific global places. A cyber secret agent network, dubbed Ghost Net, the use of servers specifically based totally definitely in China had tapped into labeled documents from authorities and private organizations in 103 worldwide places, along with the pc structures of Tibetan exiles in 2008. However, China has denied the form of claim. Again, Operation Aurora, a cyber assault which started out in mid-2009 and persisted via December 2009, emerge as first publicly disclosed via Google on January 12, 2010, and have become believed to be originated from China. The assault emerges as aimed closer to dozens of different businesses, of which Adobe Systems, Juniper Networks and Rackspace have publicly showed that they have been centered. [4]

Most presently within the twelve months 2010, Iran grows to be attacked through the use of

[4] Oredola A. Soluade, Emmanuel U Opara, "Security Breaches, Network Exploits and Vulnerabilities: A Conundrum and an Analysis" International Journal of Cyber-Security and Digital Forensics, Vol (3)4, Sep, 2014

 [ISSN 2581-5369]

the Stuxnet malicious program, belief to mainly purpose its Natanz nuclear enrichment facility. The malicious program is stated to be the most superior piece of malware ever determined and notably will increase the profile of cyber warfare.

These incidents definitely factor towards the gravity of strategies cyber conflict has come to be a superb danger to every State inside the international sphere.

IV. CYBER WARFARE IN INDIA

India is a large of the United States with international locations like China and Pakistan bordering it. In recent times technologically superior generation a mere test the scale of safety stress and navy system is not enough. Cyber conflict deterrence is likewise a few elements that we need to start thinking about. It is pleasant currently that the modern-day Indian Government moreover diagnosed the significance of cyber protection and The Department of Information Technology has in response created the Indian Computer Emergency Response Team (CERT-In) in 2004 to thwart cyber-attacks in India. In 2004 itself there were 23 said cyber safety breaches and through 2011 had risen to an alarming thirteen,301. Hence, in 2011, the authorities even created a new subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart assaults in the path of strength, transport, banking, telecom, defence, location and other sensitive areas.

An immoderate-profile cyber-attack on 12 July 2012 breached the e-mail bills of approximately 12,000 human beings, inclusive of those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organisation (DRDO), and the Indo-Tibetan Border Police (ITBP). As a response to this the Indian government did give authorities-personal area plan being overseen by using manner of former National Security Advisor (NSA) Shivshankar Menon in October 2012, whose aim changed into to red meat up India's cyber protection competencies inside the light of a fixed of professionals' findings that India faces a 470,000 shortfall of such specialists however the United States of as recognition of being an IT and software program powerhouse. In February 2013, Information Technology Secretary J. Satyanarayana stated that the NCIIPC end up finalizing policies associated with country wide cyber safety that would attention on domestic protection solutions, reducing publicity through foreign places generation. Other steps encompass the isolation of several safety businesses to ensure that a synchronized assault could not achieve success on all fronts and the deliberate appointment of a National Cyber Security Coordinator. Even these days, as gunfire remains traded across the India-Pakistan border, violating the ceasefire among the neighbours, an entire-blown hacking and defacement battle appears to have additionally

 [ISSN 2581-5369]

concurrently erupted in cyber place. The conflict at the cyber space too may be very masses on Pakistan's time desk. [5]

Pakistan like China is concept to profits cyber wars with India. The Pakistan cyber army, specifically, has been very lively at the internet and has spared no opportunity to hack into Indian web sites handiest to reason a humiliation. As consistent with the stylish alert, Pakistan has directed its cyber army to claim an internet war on India. Intelligence Bureau officials say that Pakistan will use all methods to say a non-traditional conflict on India. Like this India is usually under hazard from neighbouring and wonderful worldwide places too.

The Defence Ministry want to consequently keep in mind the advent of a Joint Command for Cyber Warfare and create warriors educated wonderful in this. It has emerged as rather vital that we recognize the gravity of those cyber wars and be aware of all of the regions of vulnerability that exist in our device. Cybersecurity tasks and obligations in India are negligible in numbers. Even if some initiatives have been proposed, they have got remained on papers handiest. Projects like National Cyber Coordination Centre (NCCC) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India, has, and so on. Didn't materialize to date. The National Cyber Security Policy of India 2013 furthermore failed to take off or perhaps if it's far implemented it's far susceptible on numerous factors like privacy violation in stylish and civil liberties infringement in particular. It won't be wrong to say that India is a sitting duck in our on-line world and civil liberties safety regime. Cyber safety goals pressing hobby of Indian government. In an amazing development, the National Cyber Coordination Centre (NCCC) of India also can ultimately see the slight of the day and might end up realistic right away. The NCCC ought to assist India is preventing in opposition to national and worldwide cyber threats. Very soon it might be clear how a way the BJP government might visit to defend Indian on-line world. We need to create both shielding and offensive talents to be prepared for such assaults. Like China, India additionally needs to construct indigenous functionality in key era in pc structures using our very own on foot structures and networking tool for our networks to grow to be regular. This attempt furthermore calls for assist from employer's as we flow in advance to privatized infrastructure like railways, electricity, and so on.

The time has now come for India to understand this want and address any vulnerability that exists within the device. In the more virtual international sphere that we're transferring toward,

[5] Jay Clayton, "Postmodernism and the Culture of Cyberspace", Published in course syllabus of Vanderbilt university, Fall 1996 course syllabus. Available at : https://www.vanderbilt.edu/AnS/english/Clayton/sch295.htm.

we need to put together ourselves to guard any net wars that come our manner.

V. INTERNATIONAL LAW AND ITS PROCEDURES TO FIGHT THE CYBER WAR

Technology has made anyone witness its height the last decade. While its miles amusing how generation can also want to make the arena enjoy related but it compliments one with an obvious evil it is the vulnerability of these systems. Earlier the concern grows to be the life of a mere virus slowing down the performance of the device which has now developed to incredibly sophisticated softwares that would cause extreme destruction no longer in reality to the machine but to human beings. From being capable of leak statistics thereby spreading rumors and inflicting panic to hacking a person's gadget for you to gain absolute statistics over all their personal facts the listing is going on. Although it has an unethical to have an effect at the people in technologically advanced nations extra the opportunities of sparing human beings dwelling in countries which can be nonetheless not simply evolved in technological phrases are not negligible.

It's an entire device of interconnected networks. All this has landed cyber protection as one in all the maximum vital worries of the times and unarguably one of the maximum referred to subjects in worldwide locations all around the international. The number one situation being the advent of a worldwide statute to regulate cyber warfare. This exhaustive article allows provide one a gist approximately what our on-line world and cyber conflict way and also examines whether or no longer cyber protection should be a humanitarian trouble and briefs approximately a few worldwide conventions and reviews coping with the same and similarly is going on to say about the stressful conditions that still desires to reap adequate hobby in regards to cyber warfare within the global place.[6]

Cyber Space

Gone are those days human beings would possibly bodily accumulate to observe a movie in a theatre or to even play a pastime. With the appearance of our on-line world, folks who accumulate together to play video games play through the usage of searching into their tool from any part of the globe. The time period 'cyberspace' turned into first coined inside the one year 1981 thru American-Canadian writer William Gibson who described cyberspace because of the fact the appearance of a computer network in an international that is full of artificially realistic beings. Cyberspace exists everywhere there can be internet. Further state Department of Defense defines cyberspace as "a global place inside the data surroundings which includes

[6] Moore, R. Cyber Crime: Investigating High-Technology Computer Crime, Cleveland, Mississippi: Anderson Publishing. (2005).

an interdependent network of statistics technology infrastructures, at the side of the net, telecommunications networks, computer structures, and embedded processors and controllers." Therefore, it could be understood due to the fact the virtual digital medium which facilitates in facilitating online conversation. It lets in clients to play video games, interact, percentage information and behavior business employer on-line.

Cyber Warfare

There exists no everyday elegant definition of the term 'cyber struggle' however the term has been interchangeably used with the time period 'cyber-assault.' Cyber struggle may be understood due to the fact the network-based totally definitely warfare through using the use of generation to break the sports activities sports of a specific country.

State with a deliberate reason of attacking the statistics systems for strategic or military abilities. The destruction might be of a couple of kinds along with targeted on the essential infrastructures of the United States which encompass their important dams or through disrupting the transportation with the resource of manner of disabling time systems or through centered at the verbal exchange machine of the country. Which could glaringly cause havoc. The most commonplace forms of cyber-assaults encompass phishing, malware attacks, denial of carrier assaults and eavesdropping. The assaults can be initiated by means of a rustic or maybe certain international businesses with the cause to harm and damage the opposite United States of America of the United States's virtual infrastructure. The crucial motive of task such assaults is to weaken the adversary's virtual shape thereby causing damage and disruption inside the whole region/state. [7]

VI. CYBER SECURITY: A HUMANITARIAN CONCERN

There are one million techniques thru which crimes arise inside the digital vicinity. Yet the global humanitarian regulation does now not boom its application till it consists of an armed war. Even in times of armed battle the statutes are not green sufficient to alter the crimes. The controversy of whether or not all the cyber sports should be included under the ambit of International Humanitarian Law appears to be a in no way finishing one despite the fact that there are slightly any few folks that may not want such an intervention. The truth that in nowadays post globalized era, there may be barely all and sundry who can live on without the net. From undue get right of entry to 1's private information to denying human beings get entry to statistics through techniques like net shutdowns, are violations of the critical human rights

[7] Moore, R. Cyber Crime: Investigating High-Technology Computer Crime, Cleveland, Mississippi: Anderson Publishing. (2005).

granted to people.

These assaults quantity to breach of confidentiality of information which finally outcomes in targeted attacks on human right activists or reporters or any such human beings worried in humanitarian paintings. An instance to help this is the Saudi authorities focused on and hacking the mobile cellphone to trap the communications amongst their dissident Omar Abdulaziz and a journalist which in the end bring about the lack of lifestyles of the Saudi journalist Jamal Kashoggi. The UN Guiding Principles on Business and Human Rights truly lays down the obligation of the private place to understand human rights and to make efforts to mitigate the damage precipitated. Yet there have been no measures referred to as for. [8]

VII. EXISTING INTERNATIONAL TREATIES TO REGULATE CYBER WARFARE

There are numerous treaties with respect to International Aviation Law, International Outer Space Law, Law of the Sea, International Telecommunications convention and the Arms Control Treaties which mentions putting a stop to cyber warfare. The UN conference on sure traditional guns encouraged the regulating of the cyber guns has been followed through the use of several countries. Further in 2001, the Council of Europe Convention had advocated that the convention should characteristic a framework to combat cyber struggle. However, the most critical drawback became that it didn't certainly speak about the big scale kingdom prepared cyber battle however just restricted to cyber-crimes like infant pornography and such others. The NATO Cooperative Cyber Defense Center of Excellence is a NATO legal navy organization which gives with subjects regarding cyber safety and its predominant intention is to sell global cooperation and art work in the direction of international cyber defense.

However, a few splendid ones which may be of use are as referred to under:

- United Nations convention in competition to transnational crime which obligated the states to undertake framework for extradition and to make laws toward organized crook groups.
- The record of the European Union Committee of the United Kingdom which tested the function of the European Union as the protective energy and moreover proposed for the advent of the Computer Emergency Response Teams abbreviated because the CERT's.
- The 2010 decision via using the UN regarding 'the introduction of an international life-style of cyber safety and taking stock of country wide efforts to defend vital infrastructure and information.'

[8] Nancy Gonchar and JoanRoper Adam, 'Living in Cyberspace: Recognizing the Importance of the virtual World in social work assessment", Journal of Social Work Education ,Vol. 36, No.3(fall 2000)

VIII. CHALLENGES TO OVERCOME

Although a present day global statute is probably a fulfillment in permitting the eradication of all of the cyber-assaults being finished to a quantity, the most number one project that desires to be addressed is the dedication of the genuine identification of the attacker due to the fact that our on-line world permits for the anonymity of the man or woman. In the digital global it is very hard to tune the real geographical vicinity or the identification of the attacker. Say even one is a hit in tracking down the attacker, the question regarding in which the prison proceedings in competition to the attacker must be initiated is an undertaking. Jurisdiction is one of the most important troubles in cyberspace. Further, all the prison tips which might be being made have to be handiest with the compliance of all of the countries which nearly is not very far from now not viable. Further some one of a kind challenge is with admire to arbitration of cyber-crimes and the way it entices the cyber criminals. [9]

Latest Technologies For Cyber Defence

The North Atlantic Treaty Organization (NATO) claims that the number one example of cyberwarfare turned into the Morris Worm incident. In 2010, the number one-ever Digital Weapon specially 'Stuxnet', this weapon focused a Nuclear Facility in Natanz, Iran. The attack became called 'Operation Olympic Games' and have become claimed to be completed thru Israel and the us at the equal time. The Stuxnet emerge as an inflamed USB power, which actually paralyzed the hardware and software application utility facilities at the Nuclear facility. Stuxnet is stated to be a laptop computer virus this is used to manipulate a manufacturing unit's meeting line. Cyber protection's fundamental motive isn't only to protect a community however it should moreover be prepared to save you, take a look at and provide nicely timed responses to any chance that could had been caused inside the past and is still a hazard to the business enterprise inside the present and to prepare for future unexpected activities. With the developing ambit of generation in extremely-modern-day days, there has furthermore been an enhance to cyber-assaults. The essential goal of cyber defence is to shield touchy information further to shield property.

IX. THE NEED FOR IMPLEMENTING THE LATEST CYBER TECHNOLOGY

Improvised Targets

Cybercrimes are not taken into consideration petty crimes. They have progressed further

[9] Raghu Santanam, M. Sethumadhavan and Mohit Virendra, Cyber Security, Cyber crime and Cyber Forensics:--Applications and Perspective, Idea Group inc.(2010)

alongside generation. Gone are the instances at the same time as cyber-crimes were a bridge to extract a small amount of cash from a person's bank account. Cyber securities are simply being used by pinnacle-notch authority's companies which include Pentagon, it is considered to be the maximum steady network, this is due to the boom inside the threat of getting hacked via an anonymous man or woman who later the government finds it tough to even tune.

Advanced cyber threats

The critical reason within the returned of the improvement in cyber defence is specifically because of the development in cybercriminals. Cybercriminals have got entry to more superior generation than any States's government has ever imagined. Moreover, the increase inside the understanding about the dark internet at the net has made it possible for cybercriminals to transport underground even earlier than certainly all and sundry notices them.

After-effects of a cyber attack

All the monetary business organization sports are associated with a common community. In fact, these days all of the commercial agency sports activities are achieved online, in a digital format, the whole lot is relying at the machine and its networks. This makes it less tough for breachers to get proper of entry to the essential information. Once the facts have been breached, it elements out a finger on the credibility of the agency, because of which the entire goodwill of the corporation or maybe a government is notably affected.

In case of the facts breach leaked through Facebook in 2018, it created havoc on social media, people commenced the #quitfacebook fashion, which forced Facebook to make some essential adjustments of their privacy coverage. It even affected the no. Of customers Facebook had earlier than and that they now have. One case of statistics breach delivered approximately questioning of all the social media structures credibility, it questioned whether or not or no longer or not each platform is much like Facebook. It made each person bear in mind whether even their private information has turn out to be being accessed through way of a person unknown?

Nature Of Cyber-Attacks

Cyber-assaults aren't quality made on Governments or on internet web websites, it's far even possible to hack a power grid of a town. Which creates public inconvenience at huge. It influences the income accumulated via the nearby municipal agencies. The device so damaged desires to be constant, the costs to repair the entire energy grid should be a massive expenditure for the nation authorities. The effect of such cyber-assaults isn't always surrounded with the useful resource of a character but they amplify to the country financial machine or even the

 [ISSN 2581-5369]

political structures. [10]

Latest Technologies For Cyber Defence

Humans created technology and in the long run it's far a person who can dispose of the era. There is not any generation that cannot be defeated. Every time era improves, there are humans accessible who reason to defeat this barricade. Hence, the super desire is to keep on adapting to changes that come our manner. Here are a few most advanced technologies in the international:

Artificial Intelligence (AI) and Deep Learning

AI is the most talked-approximately term inside the state nowadays. AI can thoroughly be used inside the software program of protection of Cyber defence. The satisfactory example of this sort of era is Google. Whenever we try to log in to our google account on a cutting-edge tool, there is -hassle authentication. This authentication works through confirming the individual's identity on the idea of two-three unique grounds. These grounds may be a few things they understand, are and function.

Deep getting to know is a totally in-depth idea of AI. Deep reading is used to verify the data. It maintains a document of all the transactions and even real-time communications that permits you to discover any virus or unwanted sports on your community.

Behavioural Analytics

After the entire Facebook- Cambridge Scandal, someone is well aware about the information being misused for behavioural assessment. This method is often applied in social media structures and on-line classified ads on the way to get the right set of target market. But this sort of technology stays below take a look at and it's far on the verge of being explored and superior for superior cyber defence technologies. This approach enables in ascertaining the sample of a machine and tracks the network interest, to right away discover a real-time risk or opportunity of a chance. For instance, a sure character's tool indicates a splendid boom in records transmission that would probably be a cyber protection breach. While this shape of era is in maximum instances used for networks, its utilization in applications and gadgets continues to be growing.

X. Conclusion

Cyber violence has increasingly end up a totally threatening difficulty of our lives as evidenced

[10] Roger W. Smith, Cybercrime - A Clear and Present Danger: The CEO's Guide to Cyber Security, Create Space Independent Publishing Platform; 1 Edition (21 June 2014).

through the incidents said above. We have become frightened of acts of cyber violence only due to the fact we've got made them acts in the actual worldwide. It come to be now not that lengthy in the past that a related computer may want to simplest touch specific connected computer structures. Now we have a unique state of affairs. By setting actual international controls on Internet-handy structures, we've got made those acts actual and threatening. Prioritizing safety over comfort is probably the most critical act of prevention. The trouble is that the human beings in the tool will take a danger for comfort and no longer absolutely understand the functionality effects. If we restrict the feasible consequences of cyber violence than the economics of the situation will maintain us pretty strong.

In nowadays worldwide, the technological advancements are at once proportional to the safety risks contained with it. Cyber-crime is an international danger which has been a fulfillment in not being capable of be regulated at a worldwide degree. Although a terrific huge form of international locations inside the international have signed treaties and implemented legal guidelines to lower cyber-attacks that proves to be no longer very enough because of the geographical versions and morality issue that differs with every area. What is probably considered criminal in a single USA won't be appropriate in every one of a kind. There is a dearth of a worldwide statute to deal with the troubles arising in our on-line world amongst countries.

In a global that is aiming at virtual sovereignty, the triumphing jail tips might in all likelihood not suffice the need of the hour. The very negligence of not taking this trouble significantly will motive intense effects on mankind destroying the peace of the sovereign international places and the human beings therein. The community connectivity of cyber-crime makes it one of the most unstable and globalized crimes. There desires to be a well-known degree of cooperation among countries in addressing these complexities most effective then can the technology serve the destiny with the top notch and now not to sell hazard thinking about that cyberspace is ever evolving.

*****

 [ISSN 2581-5369]

XI. REFERENCES

- Agamben, G. (2005) State of exception. (K. Attell, Trans.). Chicago: University of Chicago Press.
- Agre, Philip E., and Marc Rotenberg. 2001. Technology and Privacy: The New Landscape, Cambridge, MA: MIT Press.
- Anderson, R.H. And Hearn, A.C. (1996), An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After ... In Cyberspace II" (Santa Monica: RAND).
- Diamond, Jared. 2005. Collapse, New York: Penguin Group. Dickson, David. 2001. "Weaving a Social Web", Nature 414 (December): 587.
- Deutsch, Karl W. 1968. The Analysis of International Relations, Englewood Cliffs, NJ: Prentice-Hall.
- Erickson, J. 2003, Hacking: The Art of Exploitation (San Francisco: No Starch Press).
- Esen, R. 2002. "Cyber Crime: A Growing Problem", Journal of Criminal Law, sixty-six (3): 269-283.
- Farwell, J.P. And Rohozinski, R. (2011), 'Stuxnet and the Future of Cyber War', Survival: Global Politics and Strategy, fifty 3/1: 23–forty.
- Kramer, Franklin D. 2009. Cyber power and National Security, Potmac Books.

*****