Bilingual/Bi-annual Pakistan Studies English / Urdu Research Journal VOl.No.11, Issue No. 01

January--June, 2020

Iran US Relations Based on Understanding Cyber Terrorism:

By

[1]Muhammad Shah, [2]Mirwais Kasi

Abstract:

The range of the attack for Electricity Companies to cut off the electricity of their specific area or the whole state, they are capable to manage the traffic systems of the state, to manage the broader mediums and propagate their massages, to manage the military warfare weapons like missiles, radar system, air craft, and other communication systems, Train traffic system, Air traffic system, Passenger airplane, destroyed the national database system like CNIC and Passport, Satellite system, can destroyed the state Telecommunication system or hack the system, It can transfer the cash from the banks accounts, they can easily have full access to control or mange the codes of WMS equipment of massive chaos and misuse technological or medical equipment. The U.S. Russia China and other countries established a separate military commands for cyber warfare and for defense of cyber terrorism. We will work hard to show the big picture of cyber terrorism. We know that the world is in the turn of Science and technology and expertise reshape every field of our life, now also technology changes the International Relation and other sciences. The E- Government changes the way governments work, at the other hand the Social media changes the International Relations and political leaders communicate and react on the issues of the world. The behaviour of the war is now totally changed from conventional war to Cyber war. Cold war and now a day it is switched to another state, which is called cold cyber war. In the manifestation of digital technological change, the concept of State changes into a virtual states or cyber states. The world aspects the subject of terrorism just after 9/11, the International Relations of the domain and almost all stats altered the

[1]M.Phil. Scholar, Department of International Relations, University of Balochistan, Quetta Pakistan

[2]Prof., Dr. Mirwais Kasi, Research supervisor and chairman, Department of International Relations, University of Balochistan, Quetta Pakistan

foreign policies due to savage, terrorism issues and this terrorism now changed to cyber terrorism and it altered the frame work of the International Relation to challenge the cyber terrorism. We cover all the above discussion in this thesis.

Keywords: Understanding, Cyber Crime, Telecommunication System, Cyber War etc.

Introduction:

Cybercrime is a delinquent portion of Internet progress. Relating to traditional or common misconduct, cybercrime is latest in its form. Yet, the demolition cybercrime's price is not fewer than common crime.(Raiyn, 2014)

Though, the first ever cybercrime case came in front earlier in 1820. A crowd of employees of Joseph-Marie Jacquard tried to damage the loom Jacquard invented because they were afraid of losing their job to. However, adduced that is somehow distinct from the cybercrime we actually came across.(Awan, 2014)

Cybercrime we, as a layman knows, that is dependent on an interconnected network and modernized computers were found after the development of Arpanet. The first virus or infected program called, Creeper was invented in the era 1971 by a computer expert Bob Thomas(Ganguly, 2011). Whose inner intention was not based on conducting any sort of criminal misconduct Since then, infinite malicious software's were developed(Scholar, 2002).

As we are in a highly developed environment, world depends more on computer and Internet because it became the foremost part of their lives. Though the malicious software has not transformed that much, the current field has been widened all over the world. It`s the progress of our society which is responsible for making cybercrime prosper(Kadivar, 2015a).Moreover, common crime acquainted to Information Age makes us strongly adhered to our world by a concept of digitalization. Trading of Drugs, illegal trade of guns and other common crimes initiated to offer E-services, which lowers the chance of getting in front of eye and so being caught or busted(Gilmour, 2014).

Digital devotion is such order of join charge or non-avow warrior criminal to tire into the adjustment pronounce reticulation and forced difference on them to devastate the PCs, Systems Network, IT decrepit or military weapons.(Macdonald, Jarvis, & Chen, 2013) Digital insanity is the overall peril liable to be and digital holdfast is the intemperate person for the world. The internet is the universal climate or foundation to what put correspondence happens over the system. This the internet is the deliberateness of each time charge for the circle of prompt or we raise talk go off at a digression it is the on-edge standards of the state. It is

indistinguishable as atmosphere immediately meek frameworks transport rubs outside condition the usefulness of the conceivable group everywhere of supervise same the internet work in the state (Prichard & MacDonald, 2004a). The average ponders fit changed over into digital contradiction and the materialistic agitation changed over into digital psychological warfare. In such get into a physical altercation a modest bunch of state source dined digital battle be a counterpart for the reinforcement or a non-state actors like fear based oppressor can ate such assault against the state(Poonia, 2014a).
The range of the attack for Electricity Companies to cut off the electricity of their specific area or the whole state, they are capable to manage the traffic systems of the state, to manage the broader mediums and propagate their massages, to manage the military warfare weapons like missiles, radar system, air craft, and other communication systems, Train traffic system, Air traffic system, Passenger airplane, destroyed the national database system like CNIC and Passport, Satellite system, can destroyed the state Telecommunication system or hack the system, It can transfer the cash from the banks accounts, they can easily have full access to control or mange the codes of WMS equipment of massive chaos and misuse technological or medical equipment(Seissa, Ibrahim, & Yahaya, 2017). This range of gigantic attack which can easily demolish the whole state's infrastructure and collapse the country within few hours or days, it is really serious threat to the global world and we as an educationist should make people aware about this kind of violence. In this research thesis, we will explain the stages of cyber terrorism threats, their attacks and how this war can be confronted. The U.S. Russia China and other countries established a separate military commands for cyber warfare and for defense of cyber terrorism(Toregas & Zahn, 2014). Our thesis work will make people aware about this state of war so that the United Nation can take action to take control of such a war and create law and legislation for that type of combat to bar the world form this dilemma. While at the same time, it will create positive awareness to the pupils of International relation that the faces of war are changing due to technological development and cyber warfare and cyber terrorism will make a main inclusion in the chapters of the International Relation syllabus. We will work hard to show the big picture of cyber terrorism (Salleh, Selamat, Yusof, & Sahib, 2016). We know that the world is in the turn of Science and technology and expertise reshape every field of our life, now also technology changes the International Relation and other sciences. The E- Government changes the way governments work, at the other hand the Social media changes the International Relations and political leaders communicate and react on the issues of the world. The behavior of the war is now totally changed from conventional war to Cyber war. Cold war and

now a day it is switched to another state, which is called cold cyber war. In the manifestation of digital technological change, the concept of State changes into a virtual states or cyber states (Baylon, 2014). The world aspects the subject of terrorism just after 9/11, the International Relations of the domain and almost all stats altered the foreign policies due to savage, terrorism issues and this terrorism now changed to cyber terrorism and it altered the frame work of the International Relation to challenge the cyber terrorism. The Political activities, like Caro revolution based on social media massaging altered to cyber political activities. There are international law sections for cyber international law to control cybercrime internationally. Propaganda is one of the most important ponder point of International Relation but cyber propaganda to banquet and circulate the issue based on cyber space like social media(Gcig, 2015). As we know, that information plays a vital role for any triumph and revolution, Social media based on information likes/dislikes, perform the work of social survey worldwide and while at the other hand Cloud computing is the black hole for information storage every state will try to established these black holes (Cloud computing) for storage of every kind of information of other states. Mass media is one of the strong stream line of evidence which changes the state's position like news leaks as we recently observed in Pakistan and other countries i.e. panama leaks(Joshi, 2000). Recently this whole sphere is facing a problem about the social responsibility what should be the frame policies and physical boundaries in this state of globalization because it should be possible to extract latest theories and logical limits apart from physical limitations for the republics and zones. Similarly, there is a role of ICAO (International Civil Aviation Organization). The war zone Afghanistan and situation of Afghanistan war in the digital age and state of the art digital technology testing and usage at the region. The cyber combat and social media change the direction of leaders at different situation to handle the issues. The International organization growing and becoming in the form of states cyber system changes the behaviour of international organizations (Rathmell, 1997a). Religion is the issue based on which several countries make international relation but digital age is the tool to use the proliferation of religion. The UNO should set regulations for the International Relation counter the issues of the world .Cyber terrorism will be hazard for all these when a municipal or terrorist imposed the cyber war on another country, they will annoy all their systems (Heickerö, 2014). We will discuss the complete scenario of the cyber terrorism on a state level.

Scope of the Study:

The scope of this study lies into the explanation of cyber terrorism and International Relations while at the same time the association of both.

International Relations required the strong relations among the countries. Cyber terrorism is the complex problem and threat for world International Relations every state should ready for the cyber terrorism to counter. Cyber terrorism can be from state to state or non-state actor to state actor. The latest concept of Dark Net in the prism of cyber terrorism and International Relations. The international law to surround the cyber terrorism.

Cyber terrorism will be threat for all these when a state or terrorist imposed the cyber war on another state they will disturb all their systems. We will discuss the complete scenario of the cyber terrorism on a state level. At the same time what is the cyber terrorism and it is awareness on the individual and state level. This study will show the different aspects of the cyber terrorism based on International Relations.

Significance of the Study:

This examination will make the mindfulness about the cyber terrorism and the circumstance to face and handle with equipment's and method since it isn't the regular kind of terrorism or war. This war can be battled by the digital fighting specialists and PC (Personal Computer) specialists while at the other hand it can be stop by digital computer specialists. After 9/11 and other terrorists now cyber militants are getting ready for digital assaults to force on the world. This investigation will demonstrate the phases of the digital assault and the strategies how to counter digital assaults. The significance of this study that we will explain that Cyber terrorism is the emerging issue of the world part of new aspect of International Relations. The International Relations surround the new edge of technology called cyber terrorism. To explain the relation of the world new concept Dark Net and cyber terrorism. To clear the picture of International Law for cyber terrorism. We will explain the case studies of different countries specially Pakistan survey through questionnaire to show the awareness level of cyber terrorism. While at the same time amalgamation of all these concepts. This study will be novel explanation, innovative combination of phenomena that will contribute in the fields of modern terrorism called cyber terrorism. To explain the International law in the context of terrorism and counter terrorism, devising strategies for combating the terrorist banned organization. To formulate international polices/laws options for the usage of Dark Net for the betterment of peace and prosperity in the context of United Nation.

Methodology of the Study:

My plan of research is to go through the available data (either primary or secondary). And if possible carrying out interviews with the cyber terrorism and cyber warfare experts, military, intellectuals, cyber security experts, cybercrime lawyers and people, who, were somewhat or as whole involved in the cyber terrorism and warfare.

Objective of the Study:

To explore the Cyber terrorism with respect to US-Iran based relations.

Feature & Obstacles:

Cybercrime, as a new kind of crime, has many features that are more powerful than conventional crimes. These features make them more complicated for law enforcement than conventional crimes.

Internationality (Attacking on Foreign Systems):

Compared to conventional crimes, cybercrime is way faster and more powerful than the former one. For instance, the drug traffic would take days among countries, and smuggler would have enormous risk getting caught during the transportation. On the contrary, a hacker could hack one`s bank account whose country might be on the other side of the earth in a few minutes, and the risk of getting caught in action is nearly zero(Bernat & Godlove, 2012). Besides, without proper international law, hackers could walk free after conducting crime. In some circumstance, a hacker with certain knowledge of the international environment could use the relationship among countries as a shield.

High Intelligence:

Cybercrime needs certain skill set like any other crimes. However, unlike some crimes. Part of the cybercrime requires extensive knowledge in computer science. Besides that, some criminals must be able to recognize the weak spot in a large amount of codes. They need to cover their digital footprint meticulously so that they wouldn`t get caught(Yar, 2013). They need to make plans for their attacks. All these features make them even harder to be apprehended by law enforcement around the world.

Anonymity:

Sitting behind the computer, Internet users` identities are nothing but number and letters. These identities can be easily masked and altered. This feature gives people courage to do whatever they are afraid of doing in real life. Those who are bullied in real life are most likely to conduct extremely behaviour in cyber world to unleash their anger and satisfaction(Prichard & MacDonald, 2004b).

Identities give people a responsibility to their behavior. However, once the identity is hidden, the sense of responsibility drops, and people is able to conduct behavior that holds them responsible in real life. The typical example is the online racism. We can find a lot of racists` comment in online media like YouTube, but seldom in real life. In Chinese proverb: If you have nothing to lose, why shall you be afraid? Because people are afraid of losing their reputation and wellbeing in real life. Our name is tight to our reputation. Certain behavior like racism will damage that. However, once our behavior is no longer link to our identity or who we are, we become much bolder(Fuchs, 2015).

Highly Organized:

With the development of network security, difficulties of conducting cybercrime increase with it. So instead of working alone and taking all the workload, cybercriminals decide to work together and divide labour. Division of labour makes cybercrime more efficient and profitable. Generally, these groups meet in online forum. They communicate through social media or dark net chatroom. They didn`t know other`s real identities. This compartment structure makes law enforcements even harder to apprehend whole organization(Standard, 2012).

Cyber Terrorism (A Practical Side):

Cyber terrorism is a special kind of cybercrime. Cyber terrorism, by the definition of CSIS, is "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population". The only reason I isolate this crime is because it has potential to cause real casualty (Raiyn, 2014). With the development of terrorist organizations, many highly educated people joined terrorist groups. Their propaganda began to evolve from tradition media, like TV, flyers, to Internet videos, online streaming, and websites. After strict online regulation among countries, terrorists began to use deep web, also known as dark web, to recruit fresh blood and teach people how to make IED. Due to the internationality of Internet, they are capable of encouraging people to conduct terrorist attack around the world. It proves to be far more efficient than their traditional method (Raiyn, 2014). Because of the stealth and technical challenge of dark web, this kind of website are hard to shut down. ISIS is just peak of the iceberg. There are many other terrorist groups using the same method conducting crime. In some cases, terrorist groups have its own cyber division like "East Turkestan Information Center"(SANS Institute, 2014). In addition to above, if a highly trained and organized group hacks public facility, like transportation system, it will cause public panic

which will lead to a havoc. The potential damage to life and wellbeing, finance will be beyond measure.

Cyberterrorism in Iranian Atomic Program:

The disclosure in June 2010 that a digital worm named 'Stuxnet' had struck the Iranian atomic office at Natanz proposed that, for digital war, what's to come is currently. Stuxnet has clearly tainted more than 60,000 PCs, the greater part of them in Iran; different nations influenced incorporate India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany. The infection keeps on spreading and contaminate PC frameworks by means of the Internet, in spite of the fact that its capacity to do harm is currently constrained by the accessibility of successful cures, and an implicit lapse date of 24 June 2012. German master Ralph Lager portrays Stuxnet as a military-review digital rocket that was utilized to dispatch a 'hard and fast digital strike against the Iranian atomic program' (Farwell & Rohozinski, 2011). Symantec Security Response Supervisor Liam O Murchu, whose organization figured out the worm and issued a point by point provide details regarding its activity, announced: 'We've unquestionably never observed anything like this before' (McMillan, 2010). Computer World calls it 'a standout amongst the most complex and bizarre bits of programming ever created (Price, 1965). These cases are convincing. Stuxnet has solid specialized qualities. However more critical is the political and key setting in which new digital dangers are developing, and the impacts the worm has produced in this regard. Maybe most striking is the intersection between digital wrongdoing and state activity. States are gaining by innovation whose improvement is driven by digital wrongdoing, and maybe redistributing digital assaults to non-inferable outsiders, including criminal associations.

Stuxnet is an advanced PC program intended to enter and set up authority over remote frameworks in a semi-independent design. It speaks to another age of 'flame and-overlook' malware that can be pointed in the internet against chose targets. Those that Stuxnet focused on were 'airgapped'; as it were, they were not associated with people in general Internet and entrance required the utilization of mediator gadgets, for example, USB sticks to get entrance and set up control. Utilizing four 'zero-day's (vulnerabilities beforehand obscure, so that there has been no opportunity to create and disseminate patches), the Stuxnet worm utilizes Siemens' default passwords to get to Windows working frameworks that run the WinCC and PCS 7 programs. These are programmable rationale controller (PLC) programs that oversee mechanical plants. The virtuoso of the worm is that it can strike and reinvent a PC target.6 First Stuxnet chased down recurrence converter drives made by Fararo Paya in Iran and Vacon in Finland. These each react

to the PLC PC directions that control the speed of an engine by controlling how much power is bolstered to it. These drives are set at the simple high speeds required by centrifuges to separate and focus the uranium-235 isotope for use in light-water reactors and, at larger amounts of improvement, for use as fissile material for atomic weapons (Broad & Sanger, 2010). Then Stuxnet exchanged the recurrence of the electrical ebb and flow that powers the rotators, making them switch forward and backward among high and low speeds at interims for which the machines were not structured. Symantec analyst Eric Chien put it along these lines: 'Stuxnet changes the yield frequencies and along these lines the speed of the engines for short interims over a time of months. Meddling with the speed of the engines attacks the ordinary task of the mechanical control process (Chien, 2010). In a naughty touch, the worm contains a rootkit that disguises directions downloaded from the Siemens frameworks. A few media report erroneously thought the Iranian light-water control reactor at Bushehr was likewise an objective. Iran affirmed that Stuxnet tainted PCs there while denying that much harm was inflicted (Sanger, Markoff, & Young, 2010). But Bushehr appears an improbable target, on the grounds that the plutonium created by such light-water reactors isn't appropriate for weapons purposes. The more probable target is Iran's uranium-advancement program. Albeit the vast majority of the 4,000– 5,000 rotators working to date at the pilot and mechanical scale fuel-advancement offices at Natanz have been creating just low-improved uranium, similar centrifuges could be put to use to deliver exceptionally enhanced uranium for weapons. On the other hand, and in a more probable situation, it is expected that Iran could be working mystery rotator offices to deliver exceptionally improved uranium. The way to the Stuxnet worm is that it can assault both known and obscure centrifuges.

Conclusion:

Based on the cases, we can find that cybercrime is difficult to trace, and convict. My design barely provides any effort, but at least it gives hope in certain cases. It helps people who has no computer knowledge. Although countless resource has been spent on cyber security, the outcome is unpromising. Based on whole thesis and my research, we can draw following conclusions:

1. The problem with current cyber security is that it is so passive. Although countless money has been spent, we can`t win this war only by defending.
2. In spite of the fact that current cyber security measures can withstand most of cyber offenses, human negligence is responsible

for most of cyber-attacks. That is the reason that reported cybercrime cases are still going up.

As we can see from above, to fight against cybercrimes, we need many people from different fields and different countries to work together. We need to be more active in fighting cybercrimes. Countries need to put aside their differences and reach for same goal. Fighting crime should be a common goal for all countries around the world. It should not be used as a bargaining chip for international relationship. Countries should cooperate with each other in fighting crime on the base of understanding and respecting other countries` law and culture. In this way, we can achieve true cooperation rather than a formality.

One of the limitations that occur during the acquisition of various cyber security measures is a balance to be made between security measures and civil liberties. There should be also a balance between the provision of specific interests to a particular organization or government, and more general requirements for the benefit of all legitimate users to be formed an international communications and technological environment that will be unfriendly-oriented to the ambitions of cyber terrorists and extremists, cyber criminals and hackers.

References:

A Conversation With Admiral J Michael Mcconnell. (n.d.). Retrieved october 26, 2018 from https://wn.com/a_conversation__with_admiral_j_michael_mcconnell

Aboul Enein, S. (2016). Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security.

Awan, I. (2014). Debating the Term Cyber-Terrorism: Issues and Problems. *Internet Journal of Criminology*, *6743*, 1–14.

Bakshi, A., & Yogesh, B. (2010). Securing cloud from ddos attacks using intrusion detection system in virtual machine. In *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on* (pp. 260–264).

Brezina, T. (1996). Adapting to strain: An examination of delinquent coping responses. *Criminology*, *34*(1), 39–60.

Conway, M. (2006). Terrorism and the Internet: New media—New threat? *Parliamentary Affairs*, *59*(2), 283–298.

Correia, M., & Andr, F. (2009). D EP S KY : Dependable and Secure Storage in a Cloud-of-Clouds, 31–45.

Eriksson, J., & Giacomello, G. (2007). *International relations and security in the digital age*. *International Politics*. Routledge. http://doi.org/10.4324/9780203964736

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. http://doi.org/10.1080/00396338.2011.555586

Hughes, R. (2009). Towards a global regime for cyber warfare. *Cryptology and Information Security Series*, *3*, 106–117. http://doi.org/10.3233/978-1-60750-060-5-106

Impact of Alleged Russian Cyber Attacks. (n.d.). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a504991.pdf

Roberts, L. (2008). Jurisdictional and definitional concerns with computer-mediated Interpersonal crimes: An Analysis on Cyber Stalking.

International Journal of Cyber Criminology, *2*(1).

Romano, C. P. R. (2000). The peaceful settlement of international environmental disputes: A pragmatic approach. *Kluwer Law International, The Hague(Netherlands). 410*, 2000.

Slack, C., & Slack, C. (2016). Wired yet Disconnected : The Governance of International Cyber Relations, *7*(1), 69–78. http://doi.org/10.1111/1758-5899.12268

Toregas, C., & Zahn, N. (2014). Insurance for Cyber Attacks: The Issue of Setting Premiums in Context, 20. Retrieved from https://www.seas.gwu.edu/~cspri/s/cyberinsurance_paper_pdf.pdf

United States of America, Plaintiff-appellee, v. Rajib K. Mitra, Defendant-appellant, 405 F.3d 492 (7th Cir. 2005) :: Justia. (n.d.). Retrieved October 26, 2018, from https://law.justia.com/cases/federal/appellate-courts/F3/405/492/473548/

University Information Technology Services. (2010). Data Center Access Policies and Procedures, 1–9.

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*, *23*(4–6), 172–178. http://doi.org/10.1080/19393555.2014.931491

Weimann, G. (2004). *www. terror. net: How modern terrorism uses the Internet* (Vol. 116). DIANE Publishing.

Yar, M. (2013). *Cybercrime and society*. Sage.

Yunos, Z., Ahmad, R., & Mohd Sabri, N. A. (2015a). A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia. *Information Security Journal: A Global Perspective*, *3555*(May), 1–9. http://doi.org/10.1080/19393555.2014.998844

Yunos, Z., Ahmad, R., & Mohd Sabri, N. A. (2015b). A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia. *Information Security Journal: A Global Perspective*, *3555*(May), 1–9. http://doi.org/10.1080/19393555.2014.998844

Zhou, M., Zhang, R., Zeng, D., & Qian, W. (2010). Services in the Cloud Computing Era : A Survey.