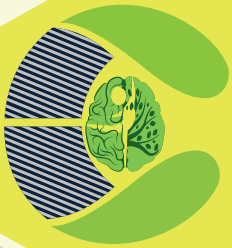
Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755

3



An Analytical Study of Deterrent Cross Domain Responses through the Cyberspace with Special Reference to India

– **Manish Manohar[1], Lekshmi Priya[2], Ciza Thomas[3], Astha Chawla[4], Pankaj Sharma[5], Abhishek Pandey[6]**

[1]manish.m1138@gmail.com, [2]adv.lekshmipriya@gmail.com, [3]ciza@cet.ac.in, [4]asthachawla1990@gmail.com, [5]p.sharma.hss18.qmul@gmail.com, [6]pandeyabhishek1103@gmail.com

ARTICLE HISTORY
Paper Nomenclature:
Argument Based Credentials (ABC)
Paper Code: CYBNMV2N9SEP2020ABC3
Submission Online: 03-Sep-2020
Manuscript Acknowledged: 06-Sep-2020
Originality Check: 07-Sep-2020
Originality Test Ratio: 13% (Drillbit)
Peer Reviewers Comment: 12-Sep-2020
Blind Reviewers Remarks: 15-Sep-2020
Author Revert: 17-Sep-2020
Camera-Ready-Copy: 19-Sep-2020
Editorial Board Citation: 23-Sep-2020
Published Online First: 30-Sep-2020

With the emergence of cyberspace as a strategic domain like the air, land and water there is a need to address the possibilities of cross-domain attacks involving cyberspace. Cross-domain deterrence involves making retaliatory threats from one domain to prevent attacks from another. Attacks on Cyber Physical Systems through cyberspace is not futuristic as evidenced from the recurrent attacks happening globally. Hence, cross-domain deterrence even though not new, has heightened relevance now-a-days. This paper includes arguments and analysis on the need for Cross Domain Deterrence based on the premise that cyber attacks are the new norm and forms a part of a broader attack on any Country. The arguments in favour of cross-domain response are presented in an analytical manner and a feasible working solution for employing Cross-domain response with special reference to India is suggested.

Keywords

- Cyber Space
- Cyber Attacks
- Cross Domain Deterrence

Introduction:

An 'eye for an eye' law of retaliation in the era of cyber attacks has involved the term "deterrence". A term which simply refers *'to prevent someone from doing something or to make someone less enthusiastic about doing something by making it difficult for that person to do it or by threatening bad results if they do it'*.[1] However, the traditional concepts of deterrence are rapidly proving ineffective in the innovative war front. The unprecedented attacks which include strategic multi-actors and multi-domains require a targeted cross-domain response to eliminate the source of the attack. The concept of cross-domain deterrence (CDD) is more relevant in the Cyberworld where cyberattacks target and immobilise specific critical resources. This warrants a response across domains to incapacitate the persons behind the attack to deter and prevent further attacks. So far, cyber deterrence has involved pulling the strings of conventional international Relations or prosecution at the International or domestic forum depending on the source of attack.

A CDD theory is vehemently opposed by some scholars as being a premise to interfere in another country's sovereignty and in escalation of conflicts. It has also been condemned for the civilian deaths which may be disproportionate to the nature of the attack. However, this opposition is futile as there is no even playing field in any of the domains. Cross domain response through cyberspace is a good option for countries who do not have great military power to tackle the threats from its enemies. This option was not available a few years

[1]*Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/deter> accessed 8 November 2020*

ago to the countries. It also levels the battle field as every country may not have the resources to fight through the same domain as the enemy. The vice-versa is also applicable i.e if one country initiates the attack through cyberspace, then the victim nation can use other domains to respond to such an attack. This was the situation when Hamas tried to attack Israel through the cyber domain and Israel retaliated by conducting an air strike against the building that was the origin of the cyber attack.

Cross Domain Deterrence: Meaning

Complex attacks employed by various actors require an equally complex solution to deter and prevent the attacks. According to the US Department of Defense Dictionary of Military and Associated Terms, deterrence refers to '*the prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.*'[2] Briefly put, a solution evolved in response to complex attacks across domains is called the Cross-Domain Deterrence. It refers to the use of a particular domain specific capability to counter or retaliate the threats, however complex perpetuated through a different domain specific capability or resource. For instance, a cyber attack is responded with an air strike. The various questions that arise, inter alia, predominantly revolves around the proportionality of the response to the attack (Asymmetric retaliation).

According to Manzo, there are two alternative definitions of the term cross-domain. It could be defined based on the difference between attacking platform and target platform or defined based on difference between target domain and intended consequences domain.[3]

Trends in cross-domain response involving cyber operations

The acknowledgement of Cyber as a critical domain necessary as part of "Cross Domain Dominance" and "Cross Domain Deterrence" has unleashed a slew of cyber attacks perpetrated by Intelligence agencies to test its frontiers by crippling critical infrastructure of other countries. The authors were faced with the difficulty of finding reliable CDD in the public domain owing to misinformation, difficulties in attribution and secrecy. However, from the available common data pool, few instances of CDD were analysed. *Table 1* summarises CDD trends in cyberspace available in the public domain.

Table 1: Trends in CDD

Year	Cyber attack used	Attacking Country (s)	Type	Target Country (s)	Motive	Attack Consequences	Cross domain deterrence
2010	Operation Olympic Games	USA and Israel	Cyber - stuxnet-malware (cybersabotage)	Iran	To deter Iran from nuclear weapons proliferation	Iran's nuclear programme disrupted	Use of cyber domain to prevent nuclear proliferation as economic sanctions and diplomatic measures failed. Cyber attack aimed to deter Iran, but Iran Retaliated with Kinetic force
2010	Flame	unknown	Cyber- Flame malware (sensitive information collection)	Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt	Unknown		
2012	Shamoon	Iran (suspected)	Wiper malware	Saudi Arabia	Retaliation for Stuxnet (suspected)	Low impact	
2015		Non-state actor: Islamic State's (ISIS) Chief Terror Cybercoach: Junaid Hussain	Hacking	U.S., U.K	ISIS propaganda	Recruitment to ISIS, instigating violence in social media and hacking, disrupting government websites and leaking sensitive information.	Targeted and killed in drone strike in Syria

[2]Department of Defense, 'Dictionary of Military and Associated Terms, Joint Publication 1-02', (November 8, 2010, as amended through June 15) <2013.https://www.cia.gov/library/abbottabad-compound/B9/B9875E9C2553D81D1D6E0523563F8D72_DoD_Dictionary_of_Military_Terms.pdf> accessed 8 November 2020

[3]Vincent Manzo, 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?' (Strategic Forum, National Defense University, December 2011) <https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf> accessed 8 November 2020

Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755

2015		China	Stealing confidential information and sensitive trade secrets through series of cyber attacks involving phishing, hacking	U.S	Stealing confidential information and sensitive trade secrets to benefit China and Chinese organisations	Stealing confidential information and sensitive trade secrets leaked	Declaration of National Emergency in US and proposed stringent economic sanctions on China
2015		Russia	Information warfare through misinformation in social media, phishing	U.S	Disrupting U.S. Elections	DNC's Presidential campaign related emails leaked.	The U.S imposed sanctions on few Russian individuals and entities.
2017	notPetya	Russia	Wiper ransomware (variant of Petya, 2015)	Global most affected are the U.S., U.K, Australia, India. Ukraine	To secure strategic benefits to Russia by undermining, retaliating against, or otherwise destabilizing: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort.	Affected very few companies	Public attribution and declared by U.K., Australia for International commitment to strengthen coordinated international efforts to uphold a free, open, peaceful and secure cyberspace The US threatened international consequences and the U.S Department of Justice charged Six Russian GRU Officers in connection with notPetya.
2017	WannaCry	North Korea through Lazarus Hacker group	ransomware	U.S., U.K most affectedIndia	Extortion, theft	High Impact: Disrupted U.K. NHS and theft of $1 million from Bangladesh's Central Bank	U.S. Justice Department prosecute, Park Jin Hyok, a North Korean Spy
2018	Shamoon	Iran (suspected)	Wiper malware (destructive variant)	Middle Eastern Countries	Disrupting energy sector of Middle eastern Countries (suspected to be in retaliation to Stuxnet)	Few Energy Sector Companies were disrupted and forced to go offline (low impact)	nil
2019		Non-state actor: Hamas terror Organisation	Attempted cyber attack , and years of surveillance, malware, phishing, honeypot	Israel	To establish Hamas's offensive cyber capabilities	Israel's Sensitive information collected and Government activities disrupted on many instances through malwares	Israel bombed Hamas Cyber operatives Base in Gaza.

The impetus for CDD began in 2010 with the "*Operation Olympic Games*". It was a joint operation by the US and Israel in response to the failed diplomatic measures and economic sanctions on Iran by the UN and other Countries to halt its nuclear proliferation. Before resorting to military coercive force, a malware called STUXNET targeting critical Industrial infrastructure used for the nuclear programme of Iran. The cyber sabotage by Stuxnet was a tactical success for the US and Israel and set back Iran's nuclear advancement.

Another secret cyber attack started in 2010 collecting sensitive information from countries such as Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt was detected by Russian security firm Kaspersky Labs in 2012. Even Though a nation state is suspected behind the attack, the complexity of the malware has deterred confirmation of the perpetrators or the real motive behind the attack such as using the sensitive information to deter or dominance.

In 2015, an example of retaliation and deterrence by a nation-state against an individual representing a non-state actor emerged. After continuous cyberattacks by senior ISIS chief recruiter Junaid Hussain, a British National, the US retaliated with an airstrike targeting and killing him in Syria. Michael McCaul, chairman of the U.S. House committee on Homeland Security of the Homeland Security Committee made it clear that the attack was intended as an "unmistakable message" of the US intentions to maintain vigilance and good intelligence to stop future plotting, and ultimately destroying the ISIS terrorist sanctuary.[4]

Again in 2015, a slew of cyber attacks by China over the years including stealing confidential information and sensitive trade secrets had the US Government planning a series of deterrent acts. In 1st April, 2015, an executive order 13694 was issued by U.S. President Barack Obama declaring a National Emergency to deal with the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States constituted by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States.[5] This order enabled the imposition of sanctions on the individuals or entities engaged in malicious Cyber Enabled activities.[6] As part of this, a public declaration was issued stating that the US has developed a package of unprecedented economic sanctions against Chinese companies and individuals who benefitted from their country's cyber theft of sensitive U.S. trade secrets.[7] This declaration came just weeks ahead of the summit between the Chinese President US President Barack Obama and Chinese President Xi Jinping. This threat of economic sanctions proved effective to deter the intensity of cyber attacks and culminated with both the Presidents taking a pledge to abstain from engaging in Cyber economic espionage.[8]

However, the long term effectiveness of this threat and pledge is questionable considering the fact that the state of national emergency has been extended in March 2020 by U.S. President Donald Trump.[9]

Also, beginning in 2015, Russian linked entities and individuals began an information warfare against the US in social media platforms with the intent of disrupting the US political system. Over the years leading to the 2016 elections, they attempted to infiltrate the Democratic National Congress by hacking. In 2016, key staff of Hillary Clinton related to the presidential campaign were targeted as part of a phishing attack and numerous emails related to presidential campaigns were stolen and leaked via wikileaks.[10] The U.S retaliated against this election interference with sanctions against few Russian individuals and entities.[11]

Another cyber attack that warranted a cross domain response is the 'notPetya' global cyber attack on 27 June 2017. NotPetya, a variant similar to Petya, was a ransomware infecting and wiping computers at many organisations. According to U.S.Department of Justice, the motive behind the attack was 'to secure strategic benefits to Russia by undermining, retaliating against, or otherwise destabilizing: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and

[4] BBC News, *UK jihadist Junaid Hussain killed in Syria drone strike, says US* (Online, 27 August 2015) < https://www.bbc.com/news/uk-34078900> accessed 8 November 2020

[5] Government Briefing, 'Text of a Notice on the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities' (*National Security and Defence*, 30 March 2020) < https://www.whitehouse.gov/briefings-statements/text-notice-continuation-national-emergency-respect-significant-malicious-cyber-enabled-activities/> accessed 8 November 2020

[6] Executive order, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities' (*The White House*, 1 April 2015) < https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m> accessed 8 November 2020

[7] Ellen Nakashima, 'U.S. developing sanctions against China over cyberthefts' The Washington Post (*Online,* 30 August 2015) <https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html> accessed 8 November 2020

[8] BBC News, 'US and China agree cybercrime truce' BBC News (*Online*, 25 September 2015) <https://www.bbc.com/news/world-asia-china-34360934> accessed 8 November 2020

[9] Supra n.7 (Gov briefing)

[10] CNN Editorial Research, '2016 Presidential Campaign Hacking Fast Facts', CNN (Online, 28 October 2020) < https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html> accessed 8 November 2020

[11] Evan Perez and Daniella Diaz, 'White House announces retaliation against Russia: Sanctions, ejecting diplomats' CNN (*Online*, 3 January 2017) < https://edition.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html> accessed 8 November 2020

Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755

(5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort.'[12] In retaliation and to deter further efforts, the US threatened international consequences and the U.S Department of Justice charged Six Russian GRU Officers in connection with notPetya.[13] Along with U.S., Australia[14] and U.K. [15]have also publicly attributed Russia for the NotPetya attack.

There are few instances of unattributable cyber attacks suspected to be sponsored by state-actors or non-state actors aided by state actors such as the 'Shamoon' cyber attack, a destructive variant of wiper malware targeting energy companies in Middle Eastern Countries surfaced in 2012 and again resurfaced in 2018.[16] However, the attribution of the attack is difficult due to its complexity, but given the political circumstances during 2012, the attack was attributed to Iran possibly in response to Stuxnet.[17]

Around the same time, in 2017, the ransomware WannaCry affected many countries worldwide, significantly, the disruption of United Kingdom's National Health Service and the theft of $81 million from Bangladesh's central bank in 2016.[18] The U.S and U.K. had attributed North Korea for the attack and in retaliation the U.S. Justice Department prosecuted Lazarus group hacker, Park Jin Hyok, an alleged North Korean spy for his role in the global cyber-attack.[19]

In 2017, Loss of human life possibly due to cyber attack was reported for the first time in Germany when the Düsseldorf University Hospital's computer systems were disabled by hackers making the Hospital unable to admit a terminally ill patient resulting in her enroute to another hospital.[20] If the pending investigations confirm the link between the hacking and loss of human life, then this will be the first incident to prove the devastating effects of cyber attack includes potential danger to human life.

The first time an immediate retaliation in cross domain for a cyberattack was documented in 2019. In this incident, Hamas terror organisation seeking to establish their offensive cyber capabilities based within Gaza strip, attempted to cyber attack Israel. Israel retaliated by bombing the Hamas cyber operatives base building as part of its cyber defensive operation.[21] This strike reportedly neutralised Hamas Cyber capabilities.[22] However, the retaliation is not in response to a single incidence. Over the years Hamas was engaged in surveillance, collecting sensitive information and disruptive tactics through cyber attacks including malwares, phishing and honeypot maneuvers. The retaliation through bombing was to put a stop to these cyber attacks and deter further attacks. If the U.S policy on cyber attacks is more geared towards Cyber dominance and Security, Israel's retaliation stands as an example for CDD.

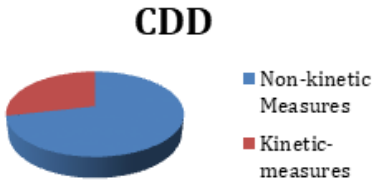


Fig 1. Employment of Kinetic and non-kinetic measures.

From the analysis of the above data and figure 1, it is evident that Cyber attacks are commonplace and are proving to be more disruptive by resulting in devastating effects felt in the physical world by putting the citizens in physical danger. Being an internationally wrongful act violating the sovereignty of a country, the cyber attacks necessitates the use of other domain forces to deter further attacks. Countries like the U.S. have been more proactive in employing CDD measures against cyber attacks. From an analysis of the data, a trend that emerges is the use of non-kinetic CDD measures such as diplomatic, economic sanctions have proved to be equally effective in deterring cyber

[12]Office of Public Affairs, 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace' United States Department of Justice (*Online*, 19 October, 2020) <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and> accessed on 8 November 2020

[13]Ibid

[14]Minister for Law Enforcement and Cyber Security, 'Australian Government attribution of the 'NotPetya' cyber incident to Russia' 16 February 2018 <https://www.dfat.gov.au/sites/default/files/australia-attributes-notpetya-malware-to-russia.pdf>

[15]National Cyber Security Centre, 'Russian military 'almost certainly' responsible for destructive 2017 cyber attack' NCSC (14 February 2018) <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> accessed 8 November 2020

[16]BBC News, 'Shamoon virus targets energy sector infrastructure', BBC News (*Online*, 17 August 2012) <https://www.bbc.com/news/technology-19293797> accessed 8 November 2020

[17]Thomas Brewster, 'Warnings As Destructive 'Shamoon' Cyber Attacks Hit Middle East Energy Industry' Forbes (Online, 13 December 2018) <https://www.forbes.com/sites/thomasbrewster/2018/12/13/warnings-as-destructive-shamoon-cyber-attacks-hit-middle-east-energy-industry/?sh=3d318e083e0f> accessed 8 November 2020

[18]Dan De Luce and Andrew Blankstein, 'U.S. charges North Korean over WannaCry, Sony cyberattacks 'NBC News (*Online*, 6 September 2018) <https://www.nbcnews.com/tech/tech-news/u-s-charge-north-koreans-over-wannacry-sony-cyberattacks-n907046> accessed 8 November 2020

[19]Ibid

[20]Joe Tidy, 'Police launch homicide inquiry after German hospital hack' BBC News (*Online*, 18 September 2020) <https://www.bbc.com/news/technology-54204356> accessed 8 November 2020

[21]Israel Defence, '**Israel Thwarts Hamas Cyberattack, Destroys the Group's Cyber HQ** ' (*Online*, 5 May 2019) <https://www.israeldefense.co.il/en/node/38418> accessed 8 November 2020

[22]ibid

attacks. Employment of kinetic force as part of CDD such as in the Hamas attack and killing of ISIS chief hacker Junaid has been a last resort measure considering the gravity of the attack or failure of other non-kinetic measures to deter future attacks.

Cost Imposition and Higher threshold on bad behavior in cyberspace.

Cross domain responses may impose lower or higher costs on the adversary. It is dependent on the kind of resources that are targeted and the dependence of the adversary on those resources. Let us take an example of two opponent parties 'A' and 'B'. 'A' initiates the attack by destroying the submarines of 'B' or any other naval command centre. As a response, 'B' could attack the fighter jets of 'A' through missiles. This is an example of a cross-domain attack involving two different domains i.e water and air. On a deeper analysis of such a scenario, few questions need to be determined as to whether by attacking the fighter jets of 'A', 'B' escalates the situation in a disproportionate manner? Was it a right move?. Some strategists look into the costs incurred by 'A' and 'B' as a metric to determine whether an action was escalatory or not. It is somewhat simple to look into the costs incurred during such attacks but what happens if the cross domain response was through cyberspace.

A question that further arises is whether it would be sufficient to have a simple analysis of the escalation tendency of a response in the cyber domain? An appropriate answer to this question requires an analysis of policies in the cyber domain. Countries do not have a shared framework to determine whether an attack amounts to escalation of conflicts. The policies regarding the escalation of an attack varies from country to country making it difficult to look into the costs[23].

The cyber domain is relatively new compared to land, water and air. Deterrence in the cyber domain seems unlikely without a shared framework. The interconnection of cyber space with other domains further complicates. An attack through cyberspace could shut off an electrical grid, destroy centrifuges of a nuclear plant (Stuxnet worm was used to SCADA systems in the nuclear power plant of Iran) and there is potentially no limit to what damages could be caused. Thus, such attacks could compound the costs on the adversary. Adding to this difficulty is the question of attribution, it is not easy to track the origin or person behind the attack in complex cases. Even if the computer resource was traced, tracing the actual perpetrators is a daunting and sensitive task. Therefore, gathering evidence for a legal prosecution is a time consuming task. Lack of evidence to attribute the attack, allows the adversary to frustrate or escape legal proceedings. This loophole is the major reason for countries breaking treaties to coordinate attacks as a response through cyberspace. In the ever increasing IoT devices dependent world, Cyber attacks are becoming increasingly fatal and millions of cyber attacks could happen on a daily basis.

One of the mechanisms called cyber deterrence through entanglement (refer Fig.1) prevents cyber attacks to a huge extent. This mechanism makes the costs of a cyber attack more than the benefits which in turn deters countries from attacking through cyberspace. For example, two opponent parties 'A' and 'B', 'A' contemplates attacking 'B' through the cyber domain. 'A' then consults his counsel members for advice on the same. They then realise that attacking 'B' could have more negative consequences as their economy is dependent on 'B'. Attacking 'B' could indirectly impose costs on 'A' or incur retaliation through economic sanctions. This prevents 'A' from attacking 'B'[24].

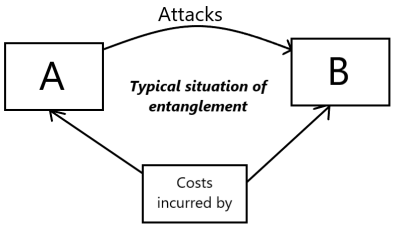


Fig 2. An illustration of a typical situation of entanglement

The costs imposed by a cyber attack are difficult to quantify as it could take a lot of time to actually understand that a person has been a victim to a cyber attack. Cyber espionage for example, could be really costly as they could steal the intellectual property of people before it has been submitted as a patent. The US has accused China on numerous occasions on similar grounds. The attacker could steal confidential information and hold it in ransom threatening to release the information on non-payment of ransom or patent the invention, process or design in his own name.

[23]Vincent Manzo, 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?' (*Strategic Forum, National Defense University*, December 2011) <https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf> accessed 8 November 2020

[24]Danzig, R., Egloff, F., Hampson, F., Herr, T., Housen-Couriel, D., Jasper, S., ... & Mallery, J. (2016). Deterrence and Dissuasion in Cyberspace. Technology, 1(1).

[23]Vincent Manzo, 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?' (*Strategic Forum, National Defense University*, December 2011) <https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf> accessed 8 November 2020

[24]Danzig, R., Egloff, F., Hampson, F., Herr, T., Housen-Couriel, D., Jasper, S., ... & Mallery, J. (2016). Deterrence and Dissuasion in Cyberspace. Technology, 1(1).

Volume - 2 Issue - 9 | September 2020 | e-ISSN 2582-5755

Let us take a look at India as an example. The cyber defence infrastructure is not strong enough. India is ranked 3rd in the world in terms of cyber attacks and threats. According to ICERT, the number of cyber attacks keeps multiplying[25]. Although India is ranked 3rd in the world in terms of military budget, it faces a lot of threats through the cyber domain and this is becoming even more relevant as India moves forward towards a digitalised system to replace the older ways of handling data. In such a case, there are two ways to tackle threats. One way would be to increase its budget allocation for cyber security or it could rely on its military capability to give a cross domain response in case of a cyber attack. Recently, on the occasion of 'Independence Day', the Hon'ble Prime Minister Shri Narendra Modi emphasised on how cyber threats endanger all aspects of Indian life. He stated that a new cyber security policy would be framed in the coming days. This shows that India is valuing cyber security more than it had ever in the past especially after there have been threats from enemy territories through cyberspace[26].

Legal implications of CDD.

Throughout the human history of conflicts, rule-based principles have been incorporated to define the limits of conflicts. While the United Nations Geneva convention and other protocols defined accepted legal and illegal behaviour for conventional conflicts, the same principles could not be applied to unconventional conflicts including cyber warfare[27].

The 'Tallinn Manual' was one of the first attempts to create broad based non-binding consensus among the international experts to create rules of engagement in cyberwarfare. The said manual as published in 2013 was later revised in 2017. The manual provides framework for use of cross deterrence methods in cyber warfare by classifying cyber offensives actions that are as disruptive as an armed attack, thereby justifying state actors to use cross deterrence offensives as they normally would in case of an armed attack[28] The manual applies the recognised international principles of national sovereignty into cyberspace[29]. For instance, if an agent of one state used a flash drive to introduce malware into cyber infrastructure located in another state the same would be considered a violation of sovereignty[30].

Before considering the legal implications under humanitarian and other laws in cross domain deterrence, it's important to understand the concept of attack and conflicts in cyberspace. The cross-domain deterrence is applicable in cases of international armed conflict and non-international armed conflict such as between a sovereign nation and a non-state actor such as a terror group or a known cyber operator of a state.

Article 48[31], 51[32] and 52[33] of the Additional Protocol (Protocol I) of the Geneva Conventions provide rules for protection of civilians. These rules offer protection and further provide guidelines for Rules of engagement (ROE) in case of conflict. Applying the said principles, similar protection is offered to civilians in the cyber domain. One could argue that the same protection cannot be afforded in the cyber-domain since a kinetic attack is very different from a cyber-attack. However, as per Article 49[34] of Protocol I, attack means act of violence in offence or in defence.

[25]Gupta, R., & Agarwal, S. P. (2017). A Comparative Study of Cyber Threats in Emerging Economies. Globus: An International Journal of Management & IT, 8(2), 24-28.

[26]https://www.livemint.com/news/india/pm-modi-says-india-to-soon-have-cyber-security-policy-11597461750194.html

[27]Richet Jean-Loup (2015) '8. Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities', in Cybersecurity Policies and Strategies for Cyberwarfare Prevention. IGI Global. Available at: http://search.ebscohost.com.ezproxy.library.qmul.ac.uk/login.aspx?direct=true&db=edsknv&AN=edsknv.kt00UM132S&site=eds-live (Accessed: 7 November 2020).

[28]Schmitt MN, "The Law of Cyber Armed Conflict," Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ednCambridge University Press 2017)

[29](Law.georgetown.edu, 2017) <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf> accessed 9 November 2020.

[30]O'Hare R, 'China's J-20 Jet Developed With 'Stolen' Plans Makes Its Public Debut' (Mail Online, 2020) <https://www.dailymail.co.uk/sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makes-public-debut.html> accessed 9 November 2020

[31]'Treaties, States Parties, And Commentaries - Additional Protocol (I) To The Geneva Conventions, 1977 - 48 - Basic Rule' (Ihl-databases.icrc.org, 2020) <https://ihl-databases.icrc.org/ihl/WebART/470-750061?OpenDocument> accessed 9 November 2020.

[32]'Treaties, States Parties, And Commentaries - Additional Protocol (I) To The Geneva Conventions, 1977 - 51 - Protection Of The Civilian Population - Commentary Of 1987' (Ihl-databases.icrc.org, 2020) <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/1a13044f3bbb5b8ec12563fb0066f226/5e5142b6ba102b45c12563cd00434741#:~:text=1923%20Article%2051%20is%20one,accompanied%20by%20rules%20of%20application.> accessed 9 November 2020.

[33]'Treaties, States Parties, And Commentaries - Additional Protocol (I) To The Geneva Conventions, 1977 - 52 - General Protection Of Civilian Objects' (Ihl-databases.icrc.org, 2020) <https://ihl-databases.icrc.org/ihl/WebART/470-750067> accessed 9 November 2020.

[34]'Treaties, States Parties, And Commentaries - Additional Protocol (I) To The Geneva Conventions, 1977 - 49 - Definition Of Attacks And Scope Of Application' (Ihl-databases.icrc.org, 2020) <https://ihl-databases.icrc.org/ihl/WebART/470-750062?OpenDocument> accessed 9 November 2020

Therefore, any acts resulting in violence either through a kinetic attack involving a precision guided ballistic missile or acts resulting in violence through implanting malware on secured civilian or defence networks would come under the definition of attack under Protocol I of the Geneva Convention. Thereby affording civilians the same protections as they are entitled under an armed conflict and same countermeasures to sovereign states to act in defence.

One of the key principles to keep in mind while applying legal principles from conventional land, air and sea-based warfare to cyber domain is effect theory. In the cyber-domain, whether or not the action per se is violent in itself is not as important as the consequence of those actions. Therefore, in the above example of civilians under Protocol I, if the consequences of a cyber act results in violence against civilians; a sovereign state would be entitled to use all measures including cross domain tools to prevent, pre-empt, defend and protect its sovereignty and citizens.

Furthermore, consequences or effects of a cyber action in terms of damage are not limited to conventional definition of harm which includes injury, death, damage or destruction but could cause more severe harms which could have far greater repercussions for a large number of people. For example, a cyber action of planting a malware in a prominent stock exchange of a country and initiating an attack on the occurrence of certain events could act like a booby trap. The 'Tallinn Manual' under rule 44[35] relies on amended Mines protocol to establish an analogy between a non-kinetic cyber-attack in case of armed conflict to laying down a mine in case of an armed conflict.

It is challenging to establish[36] and link principles applicable in conventional land, air and sea domain to cyber domain, as actions in cyber space end up creating significant chain of consequences[37]. However, a key guiding principle is consequence theory. If the objectives and consequences of an action in cyberspace are similar to consequences of an action in the land, air or sea domain, then the legal principles as available in conventional land, air and sea domain will be applicable in the cyber domain.

Cross-domain deterrence by denial and by punishment and their policy implications.

4.1 Cross-domain deterrence by denial:

Cross-domain deterrence by denial is a technique to prevent cross-domain attacks through cyberspace by having impenetrable defence mechanism[38]. The effective implementation of this technique is daunting yet achievable through a dedicated team of cyber security professionals cotionuosly monitoring the systems for any attacks. For instance, "Apple" company has established its brand as having a strong focus on security in all of its products. This campaign has made the consumers to attribute availability of strong security in its products compared to its rivals. This might dissuade potential attackers and portray an image that attacking an apple product is a costly and futile attempt.

4.1.1. Situation in India and possible implementation of Cross-domain deterrence by denial :

Cross-domain deterrence by denial can be implemented in India through guidelines or frameworks. For instance, it can be made mandatory for every single company/organisation to pass a cybersecurity test every 6 months to make sure that the company is safe. A fine must be imposed if this is not followed. A committee must be set up in every single state in the country. In order to achieve this, the cyber security funding has to be raised. There must be a standard set of rules providing the quantum of fine, circumstances for the imposition of fine, and testing procedures to be followed according to the equipment that a company has as well as its user base. The central government should regulate these policies and revise them from year to year to make sure that it is relevant. As the years pass, people will get accustomed to this procedure and cyber security would have penetrated into every organisation. Students must be taught about cyber hygiene in their schools. A study shows that 80% of the cyber attacks can be prevented by good cyber hygiene[39]. Indeed a huge number of data breaches in companies are due to spam phishing emails by fraudsters. The softwares should be patched from time to time. Every company must show that they have a clear strategy to be resilient in case it has been attacked by an adversary.

[35] Schmitt MN, "The Law of Cyber Armed Conflict," Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ednCambridge University Press 2017).

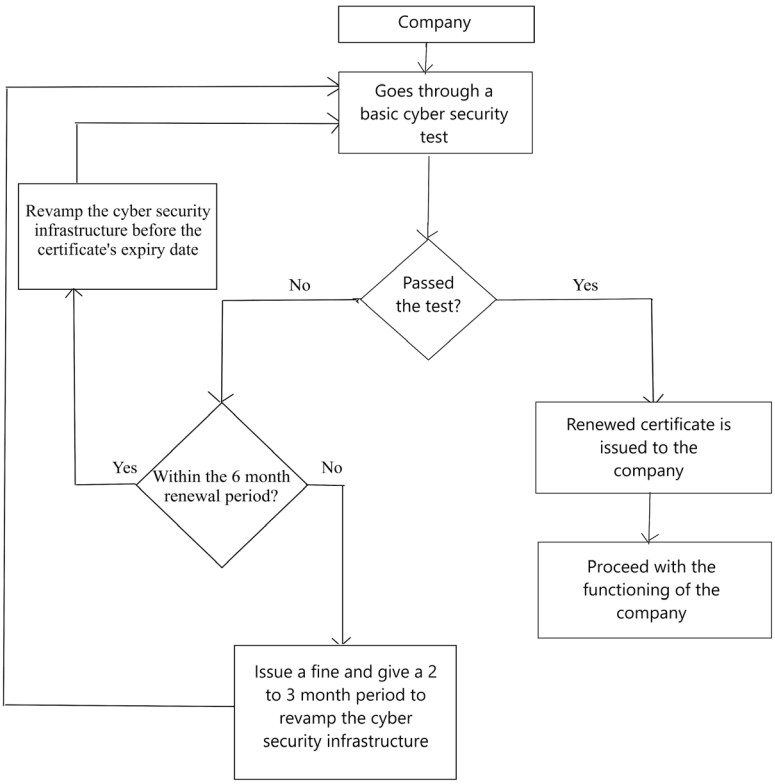
[36] 'Is Cyber Deterrence Possible?' (Media.defense.gov, 2017) <https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF> accessed 9 November 2020.

[37] 'Keep Cyberwar Narrow' (The National Interest, 2020) <https://nationalinterest.org/commentary/keep-cyberwar-narrow-8459> accessed 9 November 2020.

[38] Nye Jr, J. S. (2017). Deterrence and dissuasion in cyberspace. International security, 41(3), 44-71.

[39] https://www.nmhc.org/news/articles/cyber-hygiene-prevents-80-percent-of-breaches/ accessed 7 November.

Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755



4.2 Cross-domain deterrence by punishment:

This is a mechanism in which the cyber criminal is punished for his crime through the cyber domain[40]. If the forensics team is strong enough, it is possible to identify the criminal but it is not an easy task.

4.2.1. Current Scenario and possible implementation in India:

It is presently difficult to track cyber criminals in India. This is true for a majority of the countries. In fact, many of the cases are closed as it takes a lot of time and money to go through the procedure of law. This is especially true when there is little or no evidence to nab the criminal. Most of the time, the news about cyber criminals is usually referring to the bigger crimes in cyberspace. However, there are a lot of minor cyber crimes that go undetected such as a fake SMS that looks legitimate but is a camouflaged malware. There has to be a clear set of guidelines to determine if a person is guilty of a cyber crime. There must be special provisions to arrest a criminal with minimum evidence as it is difficult to gain strong evidence in certain cases. In case of a crime that is not involving the cyber domain, it is easy to catch the criminal by putting up photos of the criminal in many places to alert the people. In the cyber domain, evidence might lead to the computer resource used for the attack but not distinguish the human behind the attack or his exact motive. The act might be perpetuated by an innocent kid accidentally or by a hardened criminal. Another challenge that arises is the jurisdiction issues when the crime in entirety or in part be committed outside an investigating police station's or country's jurisdiction. For example, a fraudster stole money from an ATM account of a person but the ATM was located outside the jurisdiction of the police station. It could also be outside city limits. To tackle such situations, there must be a standard set of operating procedures[41].

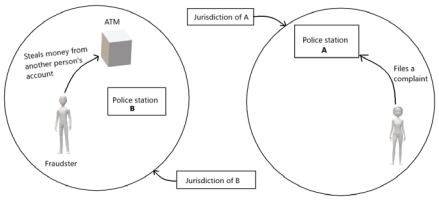


Fig 4. An illustration of a the challenge that the police faces while registering complaints

Its impact on escalation control.

5.1 Escalation Control through policy

Accessible quantitative evidence shows no signs of escalation in response to cyber operations[42] War gaming and survey experiments on different populations have also shown no signs of escalation[43].

Escalation control happens in entirely different ways because of the actors who are either cyber cynics or cyber visionaries. The cyber cynics have anxiety about collateral damage, doubt about adversary perceptions and vulnerabilities in critical infrastructure.

[40]Nye Jr, J. S. 'Deterrence and dissuasion in cyberspace. International security', (2016), Vo.14, No.3, International Security, 41(3), 44-71. <https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf> acessed 8 November 2020

[41]https://www.lawnn.com/article-cyber-crimes-cyber-investigations/#:~:text=Centralized%20online%20cybercrime%20reporting%20mechanism,mechanism%20for%20complaints%20involving%20cybercrime accessed 8 November

[42]Nadiya Kostyuk and Yuri M. Zhukov, 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? Journal of Conflict Resolution' (2017) 63(1), Journal of Conflict Resolution, <https://www.researchgate.net/scientific-contributions/Yuri-M-Zhukov-2035344842> accessed 8 November 2020

[43]Ryan C Maness, 'The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations. By Ben Buchanan.' (2018), Vol.16, Issue 4, Journal on Perspectives on Politics, Pages 1138-1139

This may lead to unintended escalation. The prime example is Nuclear C3. On the other hand, the cyber optimists have adaptable options that limit escalation by providing means to respond realistically to threats short of kinetic response.

Escalation control in cyberspace can be achieved if policymakers understand the crucial differences between non-kinetic (informational, diplomatic, and economic) dimensions in cyberspace and kinetic confrontations and conflict in the physical world. The non-kinetic dimensions being sustainable and successful have gained dominance and reputation in shaping the global security storylines. This is because of the tremendous scope that cyber-defense offers. The destructive and thus the senseless act of trying to neutralize an attacker's potential in carrying out a cyberwar and the overall uncertainty associated with any cyber-attack-defense environment must be recognized. Such offensive cyber-attacks are certainly assessed to have a high escalation potential. There may be a chain of events that start when systems are breached and may adversely result in actions like twisted bank records, intervention with military operations, or even blackouts. With the growing Internet usage and the rise in cyber-attacks, the risks arising from cyberspace are perceived significant and critical.

5.2 Escalation Control by Creating Norms

Norms are accepted guidelines of behavior that aid in escalation control. Norms help to deter catastrophes arising from confusion and lapses. An indispensable component in the implementation of CDD policy is the guarantee that both partners and adversaries will act as assured when a threshold is crossed. In cross domain deterrence, when a party joins to protect reservations or maintain a contemptuous determination not to abide by, others may be there to remind the party to obey the constraints to which they agreed upon. Thus, norms are effective at low levels of hostility and dispute. However, norms alone will not suffice when the conflicts aggravate and reach a stage of battling. Yet norms have a vital role in bolstering first-strike stability in cyberspace by both slashing benefits and boosting costs.

5.3 Escalation Control in India

India's policy has always bordered on a preference of less disruption and violence. It is true that the escalation risks from India's cyber-operations is totally dependent on the viewpoint of others. In the phase zero operations when India is ready to organize the cyber war front by assessing possible targets and attacking them with malware, or strengthening its own defenses, it is necessary to stay invisible to reduce any sort of risk. Such operational cyberwar against targets that are hit by kinetic attacks tend to escalate the tension when the other side retaliates the cyberattacks. In such situations, the deliberate cyberwar might well likely become a vicious circle of attacking and retaliation escalating tensions without a physical attack. Retaliatory strategies can often be a way to manage the other side's escalation and the linkages between purpose, influence, and awareness are rather weak in cyberspace. Other nations can be allowed to participate in this cyberspace because the basic means are available and geographical distance is irrelevant. If a persuasive nation carries out cyberattacks for us, then certainly the target nation will consider the practicality of responding to such attacks. This may be true even in the case of symmetric conflicts, and it is expected that the third-party attacks lend caution to responses and help in escalation control. Escalation control demands foreseeing how the other nation will react to our actions. It is necessary to be careful and have at least a shaded understanding of other nations.

5.4 Defensive Stability through Escalation Control

It is necessary to identify whether the existence or at least possibility of cross domain cyber deterrence threatens defensive stability. As there are many other factors that contribute to instability in a defensive system, we are inclined to vote in favour. The kinetic attacks can be perceived as enormously destabilizing because it renders the target's capabilities totally harmless by destroying it.

At the same time, the acts that make kinetic instability an issue do not necessarily carry over to cyberspace. It is worth noting that the physical world itself is affected with the experiential consequences of any cyber-attack. It is seen that even a nuclear-armed nation might yield to the will of another nation that is non-kinetically powerful. It is not that cyber-attacks cause the physical forces to cease existing, the adversaries may find it hard to be adequately confident that they have disabled all forms of adversary kinetic powers to the point where they can then act with immunity. Also, it is important to understand that no nation can neutralize the cyber capabilities exclusively through a cyberwar. A cyberwar may destroy systems, deny access to the Internet, harm and demotivate hackers; but not simultaneously. However, as cyber-defenses can never be perfect, and thus are not inherently destabilizing. It is only the arms races between offense and defense that have traditionally fostered instability. It is difficult to know the vulnerability of a well-protected target system and hence the success of offensive techniques are unpredictable. The best response

Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755

to an offensive cyber-attack is to fix the vulnerabilities in one's own system that allow such cyber-attacks to work[44].

The cost of developing aggressive and offensive cyberspace skills are reasonable when its benefits are enormous with lopsided risk to an adversary. In disagreement, the escalation control can happen due to uncertainty in cyber-space and the connected risk aversion. Self-deterrence from acting in some of the new domains is again because of the ambiguity in the magnitude of the adverse effect that it might create. The risk aversion is also contributed due to factors like complete vagueness of the adversary's cyber capabilities, paired with swift technology advancement that may cause an attacker to be clueless of their own success rate. It is welcoming that actors underestimate their competences and overestimate the proficiencies of their adversaries resulting in defense stability.

Potential Solution framework with respect to India

According to NITI Ayog Report, India ranks third globally in terms of Internet user base.[45] This is dangerous in light of the fact that India ranks third among nations facing cyberthreats in 2017 according to Symnayec, an online security software firm.[46] In Spite of the existence of defence mechanisms, research centres and laws and regulations in India, these attacks have proved that India defences are easily penetrable. India needs to strengthen its emphasis on recognising Cyberspace as a new warfare domain and the cyber attacks are a part of a broader attack such as a possible full fledged aggression or war. In such a broader integrated or hybridized attack, zero exercise of CDD can be at best termed as an utopian context in the current scenario. India needs to employ CDD based on the impact or capability to zero in on target with minimal civilian loss. Making each country's cyber domain impenetrable is a futuristic vision especially when countries are plagued with external and internal aggression. In such an event merely resorting to the same domain attacks is futile especially in the event the attacking country's cyber capabilities is stronger than the target country's. Cost of cyber attack is comparatively smaller when compared to the cost of identifying and strengthening vulnerabilities in terms of both money and time. Thus resort must be to cross domain approaches to deter further attacks. For instance, a small island nation may have stronger cyber capabilities compared to its target country. However, if the target country's military capability is stronger, the only possible logical solution will be to eliminate the source of the attack as part of its retaliation strategy to deter future attacks. This proves effective rather than spending time during attacks to strengthen vulnerabilities leaving the floor open for continuous attacks on its vulnerabilities or improving the attacking country's cyber capabilities. This is more relevant in times of war. A retaliation in the same domain cannot guarantee stronger damage to be a deterrent. But a cross-domain retaliation can guarantee stronger impact and send the message loud and clear to deter any future attacks.

On an analysis of the available literature and data of CDD, it is evident that a generic solution to cyber attacks is impossible considering the frenzied innovation in cyber attacks. Each complex attack requires an equally fresh and tailored innovative attack or countermeasure utilising a different domain capability or same domain capability depending upon the situation. However, inferences can be drawn from known cyberattacks and cross-domain responses to cull out a workable solution for different scenarios. India must learn from the experience of others and a staggered approach to using CDD measures will benefit India.

Identifying a proportionate response to cyber attack is a frustrating process in futile as it is very subjective or a country may lack the technical expertise. India needs to build capabilities in cyber, military and other related domains that itself acts as a deterrent by showing:

1. Defences are costly to infiltrate
2. India can retaliate and sustain in a prolonged war making the attacking Country think twice before attacking India (not a quick victory)
3. Develop diplomatic ties to be able to secure allies or enforce economic or trade sanctions.

Thus, a resort initially must employ diplomatic, legal prosecution, trade and economic sanctions as a non-kinetic CDD measure. A public attribution of cyber attack must be followed as in the case of NotPetya Attacks, this could act as a deterrence by portraying that India will not tolerate cyber attacks. If such non-kinetic CDD measures fail, the most logical response is the kinetic CDD response. However, before resorting to Kinetic CDD measures, an identification of a retaliatory threshold limit for employing CDD measures is necessary to prevent unnecessary escalation of conflict. Simultaneously, the infrastructure and cyber capabilities of both the private

[44]Vincent Manzo, 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?' (*Strategic Forum, National Defense University*, December 2011) <https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf> accessed 8 November 2020

[45]Dr. V.K.Saraswat, 'Cyber Security', Niti Ayog Report, 2019 <https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf>

[46]Ibid

and public sectors must be upgraded with stricter emphasis on cyber hygiene. Any cyber attack on India must be deterred considering the level of defence in place and the heavy cost and negligible impacts that might result in continuing with the attack. Investment in shoring capabilities is a successful deterrence only when a will to act or react to cyber attacks is expressed by a country.

On the technical front, an isolation of the network must be encouraged to prevent the spread of malwares and cyber attacks such as the Aramco Saudi oil Corporation employed to prevent further shamoon attacks. Similarly, a strong co-operation between Private and public sectors must be achieved to share information and coordinate mitigation and defending efforts against an attack. Cyber hygiene must be the norm and penalties imposed for any laxity. Cyber Hygiene must be maintained at all stages of attack. India must facilitate its critical infrastructures (cyber-physical systems) like Defence facilities, Power infrastructures, Hospitals etc. with strong attack detection capabilities. Along with this, focus should be laid on attack prevention techniques for such infrastructures. Thus when India emphasises aggressively on the cyber security aspect of different facilities this would increase the cost of attack for attackers in terms of their efforts or sophistication level involved and thus deter them.

Also, on the Human resources terrain, all staff, especially in the public sectors, must be educated through additional course or awareness campaigns to detect cyber attacks and the procedures to be followed during and after attacks such as preserving, mitigating, and reporting attacks. The staff and companies must be trained to expect cyber attacks and isolate any unusual activities.

On the international level, India must continue to develop and strengthen diplomatic ties. India must coordinate with countries to eliminate targets or potential cyber attacks or resources. These relations can aid in times of imposing economic or trade related sanctions on the attacking country. This could potentially act as a deterrent, when a united front is shown to the attacker signalling a heavy impact on the economy and social status of the attacking country.

Only with updated cyber capabilities and weeding out vulnerabilities across all sectors can India put a strong firewall that can show that India can withstand a sustained attack and also is willing to retaliate. A perfect solution for deterring cyber attacks does not exist, however, by shoring up the defence mechanisms and plugging the vulnerabilities, a tailored solution for each new attack can be found and used to eliminate or mitigate the attack.

The authors argue for the employment of Cyber Deterrence Technique in a phased and holistic manner to avoid escalation of conflicts or minimise the use of Kinetic forces until as the last resort. This is suggested keeping in mind that India has not achieved cyber resilience to withstand sustained cyber attacks in retaliation to use of force by India retaliating previous attacks. Any disruption in cyberspace will prove costly for India. However, when push comes to shove, India has to resort to Kinetic measures to prove that it is not an easy target and has the capacity and determination to deter future attacks. Thus, a staggered CDD measures in cyberspace will give India a fighting chance by deterring cyber attacks.

Conclusion

The recognition of cyberspace as a new domain has opened up a pandora's box of twisted questions. The most prominent of all is the question on the utilisation of CDD techniques in response to cyber attacks. On an analysis of all the aspects of CDD, it is evident that a tailored CDD is requisite to level the playing field with respect to each attack. However, an universal solution for the application of CDD is impossible as the cross-domain deterrence decisions are context dependent based on the impact, motive or complexity of the attack. The cybersecurity infrastructure, policies and guidelines should be impeccable and flawless to prevent escalation of conflicts or mitigate or neutralise cyber attacks. India as a country is progressing in the digital world rapidly and to prevent any setback or threat to its national security, it has to strengthen its defences, keep its allies close, educate its personnel, monitor attacks and set in motion a mechanism that can be employed during and after attack.

Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755

Manish is a student currently in the third year of his undergraduate programme in 'Computer Science and Engineering'.He is very passionate about the field of Cyber security.He is currently a research intern at Samsung Research Institute, Bangalore.He has completed internships in android app development and web development.He loves to keep gaining new skills in his journey.

manish.m1138@gmail.com

Lekshmi Priya L is an Advocate at the Madras High Court, Chennai and is associated with CEERA, NLSIU as a research assistant. She is pursuing her master's degree in Law from TNDALU, Chennai and PGD in Cyber Law and Forensics from NLSIU, Bangalore. She has completed an International Arbitration course from LSE, London. She has secured top positions in several prestigious National Moot Court competitions, debates and published articles on various legal topics. She has a keen interest in exploring the nuances of law.

adv.lekshmipriya@gmail.com

Ciza Thomas is currently working as Senior Joint Director at the Directorate of Technical Education, Government of Kerala. She completed her B.Tech and M.Tech from College of Engineering Trivandrum and PhD from IISc, Bangalore. She was trained in Cyber Security at the Computer Emergency Response Team (CERT) at US and also at Carnegie Melon University, Pittsburgh, US, under Govt. of India scholarship. She has publications in more than 60 International Journals and International Conference Proceedings. She has edited eight books and published fifteen book chapters in the field of network security. She is a reviewer of more than fifteen reputed International journals. She is a recipient of achievement award in 2010 and the e-learning IT award in 2014 from Government of Kerala. .

ciza@cet.ac.in

Astha Chawla is a Ph.D. research scholar in the Department of Electrical Engineering, Indian Institute of Technology Delhi. Her research interests include the security of cyberphysical smart grid systems, synchrophasor technology, and artificial intelligence applications in power systems. She has worked at Faculty Position in MNNIT Allahabad in 2016-2017. Chawla received an M. Tech. in Instrumentation and signal processing from the Electrical Engineering Department, Indian Institute of Technology Roorkee in 2016.

asthachawla1990@gmail.com

Pankaj is an Ad-hoc Arbitrator, Advocate and presently serves as counsel for the GNCTD. He's a Chevening Scholar and has LL.M from Queen Mary University of London and LL. B from Faculty of Law, University of Delhi. His areas of interest involve interdisciplinary fields of law and technology including competition-IP, e-commerce transactions, arbitration, privacy and, cybercrimes & digital investigation regulations.

p.sharma.hss18.qmul@gmail.com

Abhishek is working as an cyber security engineer at CyberSmithSecure. His areas of interest are digital forensics, OSINT, Social engineering, and incident response.

pandeyabhishek1103@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
03-Sep-2020	195887	8221	44945

DrillBit Anti Plagiarism Software

13 SIMILARITY %

50 MATCHED SOURCES

B GRADE

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

SLNo	LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1.	2	link.springer.com	2	Internet
2.	1	deterrence.ucsd.edu	2	Publication
3.	4	www.rand.org	1	Publication
4.	12	media.defense.gov	1	Publication
5.	7	link.springer.com	1	Internet
6.	22	Data for free Using LMS activity logs to measure community in online by Eri-2008	<1	Publication
7.	20	The Balance of Terror Torture, Terrorism, and Security, by Campbell, K.- 2007	<1	Publication
8.	38	www.frontiersin.org	<1	Publication
9.	33	Student Report Submitted to Bangalore University by - '161GCMD097' Yr - 2018	<1	Student Paper
10.	16	heinonline.org	<1	Internet
11.	21	Coordinating a Multi-Platform Disinformation Campaign Internet Resear by Lukito-2019	<1	Publication
12.	29	www.nationalreview.com	<1	Internet
13.	9	arpgweb.com	<1	Publication
14.	30	www.rand.org	<1	Publication
15.	6	The cyber threat landscape Challenges and future research directions by Kim-Kwan-2011	<1	Publication
16.	39	Project termination practices in Indian industry a statistical review, by P.K. De- 2001	<1	Publication
17.	3	Cohesive Soil Stabilized Using Sewage Sludge AshCement and Nano Alumi by Luo-2012	<1	Publication
18.	8	www.jstage.jst.go.jp	<1	Publication
19.	37	Fancy bears and digital trolls Cyber strategy with a Russian twist by Jensen-2019	<1	Publication
20.	28	www.frontiersin.org	<1	Publication ()
21.	25	IEEE 2015 IIAI 4th International Congress on Advanced Applied Inform by	<1	Publication
22.	50	Inclusion and Diversity in Work Groups A Review and Model for Future by Shore-2011	<1	Publication
23.	35	Working towards HIV prevention choices for women by va-2017	<1	Publication
24.	45	www.citizenrobo.org	<1	Internet
25.	27	www.cisuc.uc.pt	<1	Internet
26.	14	www.intechopen.com	<1	Internet
27.	26	www.frontiersin.org	<1	Publication
28.	17	doctiktak.com	<1	Internet
29.	34	fas.org	<1	Publication
30.	13	A multi-objective decision model for regional development, environment by A-1976	<1	Publication
31.	42	www.frontiersin.org	<1	Publication
32.	18	Reparations After Identity Politics by Balfour-2005	<1	Publication
33.	15	State, Song, and Shabb in Syrias Prewar Radioscape by Bothwell-2018	<1	Publication
34.	40	www.jbc.org	<1	Publication ()
35.	24	downloads.hindawi.com	<1	Publication
36.	19	www.infopig.com	<1	Internet
37.	47	Role-based access to facilities lifecycle information on RFID tags by Al-2011	<1	Publication
38.	41	Scores Identify Subsets of Mild Cognitive Impairment with Var by Royall-2019	<1	Publication
39.	11	research.ncl.ac.uk	<1	Publication
40.	43	www.arxiv.org	<1	Publication
41.	23	www.frontiersin.org	<1	Publication
42.	44	justcoachit.com	<1	Internet
43.	5	farname.ir	<1	Publication
44.	49	There is no mystery to sleep, by Foster, Russell G.- 2018	<1	Publication
45.	48	arxiv.org	<1	Publication
46.	46	Thesis submitted to shodhganga - shodhganga.inflibnet.ac.in	<1	Publication
47.	32	www.oecd.org	<1	Publication
48.	10	www.federalregister.gov	<1	Internet
49.	36	www.communitybanking.org	<1	Publication
50.	31	IEEE 2019 International Colloquium on Logistics and Supply Chain Man	<1	Publication

Note: The Cybernomics had used the DrillBit plagiarism [https://www.drillbitplagiarism.com/] tool to check the originality.

Volume - 2
Issue - 9
September
2020
e-ISSN
2582-5755

Reviewer's Comment 1: The article is very well drafted and presented in a comprehensive manner by highlighting all the relevant arguments and with supporting examples in the context of the theme.

Reviewer's Comment 2: The theme of the study is very new and relevant in present time, which has not been explored much. The study provides the basis to other researchers for further research in the area.

Reviewer's Comment 3: The arguments in the paper are very well supported by taking examples across the world, which improves the reliability of the study. A good number of references are used.

Editorial Excerpt

The article has 13% plagiarism which is an acceptable percentage for publication. The comments related to this manuscript are noticeably related to the theme "Deterrent Cross Domain Responses Through the Cyberspace" both subject-wise and research-wise. Cyber attacks are the new norm these days and form a part of a broader attack on any Country. By taking evidence from the recurrent attacks happening globally, attacks on Cyber Physical Systems through cyberspace is not futuristic. This paper includes arguments and analysis on the need for Cross Domain Deterrence. After comprehensive review and suggestions by the editorial board the paper has been categorized under the "**Argument Based Credential**" category.

Acknowledgement

The authors are highly indebted to Scholastic Seed Inc. and publishers of Cybernomics Magazine & editorial team including Resident Associate Editors (Ms. Sonakshi Jaiswal, Ms. Jyoti & Ms. Shailza), for making the write-up in the shape of an article.

Disclaimer

All the views expressed in this paper are my own, of which some of the content is taken from open source websites for knowledge purpose. The content drawn from different sources have been mentioned above in the references section.

Citation

Manish Manohar, Adv. Lekshmi Priya, Dr. Ciza Thomas, Astha Chawla, Pankaj Sharma and Abhishek Pandey

"An Analytical Study of Deterrent Cross Domain Responses through the Cyberspace with Special Reference to India" Volume-2, Issue-9, September 2020. (www.cybernomics.in)

Frequency: Monthly, Published: 2020
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in
https://orcid.org/0000-0002-7952-096X