iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46645

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Cross-Domain Deterrence in the Cyber World

Amit Lambi[1], Sandeep Vijayaraghvan[2]
[1, 2]*REVA Academy of Corporate Excellence, Bengaluru, Karnataka, India*

Abstract: ***Cyber Space, like outer space, is strategically a vital domain for state offence and defence. However, there has been a substantial rise in the sponsored cyber activities to inflict heavy losses to critical infrastructures due to the lack of rules or norms or any strict international regulations to govern the conflicts in cyberspace. This activity affects the national defence strategies when oppressed by the response crisis and hugely impacts the risk factors. In these circumstances, the dilemma is whether any operative or offensive choice in the event of a cyber threat or cyber-attack violates international law.***
War has always been a last resort when other forms of punishment have failed, but the power dynamic has fundamentally shifted since World War II. State Governments have been hoarding the arsenals that could destroy cities in a second; hence a need for unconventional resolution has led to the evolving nature of deterrence. States must reconsider alternate strategies to protect their sovereignty by implementing cross-domain deterrence that can cripple an adversary economy, swift surgical strike as retaliation, or curb the attack using counterintelligence. The threat landscape in Cyber Space is beyond frontiers, and the consequences cannot be contained at the perimeter by the regular armed forces. Require special forces and strategies to mitigate the risks. Cross-Domain deterrence to increase cyber resilience, it is crucial to identify existing strategy disparities to take necessary actions on the state misconduct and the misconduct of a policy for global cooperation during state-sponsored cyber-attacks. This paper discusses the evolving framework by assessing the changing threat landscape and its associated risks.
Index terms: Cyber-space, Cyber-Resilience, Geopolitical influence, International Law, Cyber-Deterrence. Cross-domain, Cyber defence, Cyber-Norms, CIA Triad.

I. INTRODUCTION

Offensive cyber capabilities are on the rise. If any country uses this capability to attack the critical infrastructure of another state, disrupting essential services and leading to loss of life, the pressure to retaliate would be very high. It may set off a domino effect of destruction. In this scenario, avoiding any harm in the cyber world through deterrence involves the threat of punishment, retaliation in case of damage, denial that includes strong defence, raising the cost of implementing the attack itself, and normative considerations that can incur reputation costs. In the book The Strategy of Conflict, Thomas Schelling states that defeating your opponent is not enough; instead, opportunities to cooperate must be seized, which could involve everything from deterrence, limited war, disarmament, and negotiation. For example, India's actions depend on its calculation of Pakistan's reactions and vice-versa. This strategic interdependence provides the logical theory to understand intra-state behaviour in a cyber war. The use of threats is to deter or compel an adversary. At the same time, military capabilities offer the power to bargain. We now know that nuclear weapons are more of a deterrent than a solution.

II. DEFINING CYBERATTACK

Cyber-attacks may steal data, modify information, or destroy infrastructure by installing spyware, slag codes, or a DDOS attack. There is a fine line in terms of "cyber-attack," "cyber-warfare," and "cyber-crime" that are used without any clarity, making it challenging to design a robust legal framework. "Attack", on the other hand, is any hostile activity such as espionage, sabotage, or mere penetration. According to Richard Clarke, cyber-war is "actions taken by a state to infiltrate another state's computers or networks with the intent of causing destruction or disruption." Legal experts agree that to qualify as an armed attack or use of force involving military or intelligence operations under international law. A cyber-attack must result in death or significant injury to persons or property damage. They are attempting to limit the term "cyber-attack" to incidents causing physical harm, thus distinguishing it from common data breaches [1].

III. DETERRENCE THEORY IN CYBERSPACE

Deterrence in layman's terms means "Discouraging an attacker by making him believe that the cost incurred will be higher than the expected gain from the attack." If we look at deterrence through the lens of the CIA triad, we realise the importance of Integrity and Availability. Breach of confidentiality usually occurs through cyber- espionage sabotaging Critical Infrastructure, thus affecting the day-to-day lives of its citizens. Such attacks bring in damages both in terms of economic loss and fatalities. International norms of war dictate that retaliation should be proportional to the harm suffered from the attack.

Deterrence of these attacks is of absolute priority in the cyber domain; however, in a world where espionage has become a norm, the matter hardly escalates beyond diplomatic actions, thus questioning the existence of effective deterrence. As the nature of cyberspace provides anonymity, an attacker can easily hide behind proxy actors impersonating other states leading to problems of "Attribution." Even if the will to retaliate remains, the Attribution issues question the "timely detection" aspects. The strategic bilateral agreements between nations often enable tracking the attack's origins. However, the same context of international relations can also be used as a tool of deception by the adversary state [2].

With the advent of artificial intelligence, deception would be more proficient, increasing the complexity of Attack Surface Cyber-Attacks, Technique Adaptation, Tactical Adaptation, and Adapting to a Changing Defense Ecosystem. These evolving technologies can make all sorts of counterintelligence measures completely ineffective. The WIPO study on technology trends in A.I. research found U.S. and China to be the top players in A.I. patent filings. Such situations can render few states extremely resilient to deterrence and therefore sabotage the Deterrence theory in its present form [3]

IV. NEED FOR THE CYBER REGULATION POLICY

Every country frames the policy with their self-interests in mind. Many issues such as Attribution, differentiating hostile attacks from innocent mistakes or ambiguity on what establishes an attack under international laws undercuts cyber deterrence. This poor reliability of retaliatory threats would be accessible by the expression of requisite solid international norms that distinguish legal from illegal behaviour and expedite the punishment of cyber assailants. Analysis of cyber-attacks to know what is governed by the law of war and other existing law bodies is of prime importance. The United States of America has a monopoly on internet control, and its allies in Europe strongly support the adoption of the Budapest Convention. However, countries that fear the dominance of the USA have come up with their convention led by Russia at the U.N. General assembly. This squabble has made us fully understand that reaching an agreement on an all-nation policy can be a long-term undertaking that may become obsolete as cyber technology advances. Thus it is critical to have a guideline for the nation to follow or a mutual bilateral agreement between countries for cooperation. When State-on-state cyber-attacks escalate unpredictably owing to the lack of regulatory protocols, the international association for evidence collection, information sharing, and criminal prosecution of those involved in cyber-attacks will be essential for a proactive legal response. An excellent example of international collaboration could be the bilateral agreements between the USA and China when both Presidents agreed that their governments would not conduct or knowingly support cyber-enabled theft of any intellectual property for its advantage on the 25th of September 2015. As per a FireEye assessment, Cyber offences in the USA decreased after the Obama –Xi agreement [4].

V. A MULTI-PARADIGM COMPREHENSIVE FRAMEWORK

For designing the cyber-security policy, it is essential to have a framework defining the severity of cyber incidents. This framework would evaluate the effect as observed, its impact, sectors affected by the attack, and Attribution, if available with the state. The significant ladder in severity is likely to impact the state's public health, national security, civil liberties, economy, and law & order. To create a comprehensive framework for cyber regulation, we must think about it in several paradigms and use various tools. Our proposed framework shall have two distinct paradigms of action and three different tools to achieve a framework that can provide for the need for a robust response to a critical Cyber- attack scenario. The tools we intend to use are our Resilience, Deterrence, and Norms. Our framework shall include two paradigms, namely International and individual state actions. The framework is on the attack categorisation into four levels of transgression [5]. Achieving technical superiority has been an observed behaviour of states for decades now. Resilience is about gaining immunity to possible cyber-attacks from prospective adversaries. Due to a massive gap in technical capabilities, deterrence can become relatively ineffective [6]. As a result, resilient measures must be implemented. To absorb the attack and ensure business continuity. A comprehensive framework of action and analysis readily available to develop standards in critical attack scenarios is the need of the hour. Individual states and corporates can take two steps: resilience and deterrence. Norms are a way forward to call for international collaboration in finding and punishing the adversary. Framework design tools include Resilience, Deterrence, and Norms.

A. Resilience Measures

There is a dire necessity for states to promote research efforts in building Fault-Tolerant Critical Infrastructures in terms of technical and human accountability. Robust counterintelligence measures and Rapid Action Forces can help timely detect cyber-attacks to undertake effective incident response measures. Standing up after the damage to give a tight fist could help the state achieve its aim of future deterrence. Resilience is beneficial in reducing the benefits of the adversary.

To fortify the entire government or nation, private and academic entities must contribute alongside the government. PPP model and educational research groups funded by government and private organisations can help build a solid and robust defence. Many cybersecurity firms have used their expertise in forensics and cyber-attack investigation to identify the attacker contributing to a robust cyber domain.

B. Deterrence Measures

Cross-Domain Deterrence can be across four domains: nuclear force, Physical force, Cyber force and Diplomatic and Economic Actions.15 The USA has officially stated its right to respond to critical cyber-based attacks as an act of war. NATO has labelled cyber-attacks as actions that could activate "Article 5 of the Washington Treaty," i.e., the response through the conventional military. Apart from Diplomatic, Information, Military, and Economic (DIME) measures, other political mechanisms such as diplomatic talk take the first course, followed by Entanglement, which is used as a political tool to induce discussion such that a successful attack will impose an equal and severe cost on the attacker due to interdependence. A classic example of this is in 2009 Chinese communist party was asked by the people's liberation army to sell off China's foreign holdings to harm the USA as retaliation for selling arms to Taiwan. But China's central bank rejected this suggestion claiming it would impose a high cost on China [7].

C. Norms As An Effective Alternative To Hard Law In The International Community

Observed behaviour in the past few decades suggests that norms could play a significant role as an alternative to Hard Law. States often abide by the means adopted by the international community to build confidence in their favour. In general, behaviour is used for taking adequate measures to achieve cyber hygiene and improve the capabilities of Attribution and forensics. The U.N. Group on Information Security adopted a Consensus Report in 2013 (amended in 2015), which implies that cyber operations that amount to a "use of armed force" shall then abide by the same rules that apply for "kinematic warfare." 19 Thus, it confirms that "international law and Charter of the U.N. " applies to cyber activities.

VI. THE SEVERITY OF THE INCIDENT - METRICS FOR ECONOMIC DAMAGE AND FATALITIES

The severity of an incident can be assessed based on the revenue loss faced by the victim country due to cyber-attack crashing stock prices or initiating economic crises—possible categories in which the severity of transgressions could be assigned depending on their impact and cost. "Heedless" is one such category in which there is a lack of regard for the consequences of the attack. Transgression of these categories may behave like a domino or can have a cascading effect in which it may affect way beyond the intentional damage. Heedless mainly affects the target, but that target can be critical and can be a catalyst for further damage. An example of heedless transgression is the WannaCry attack which had widespread effects. Another category is "Brazen," in which attacks can cause death or physical destruction or defy international norms of war. Cyber-attacks have scope, duration and intensity associated with it. But if it crosses the threshold framed by the state, it comes in the category of brazen transgression. Two examples of brazen transgression can be espionage to steal employee data with less intensity. Still another example could be the Stuxnet attack in which the USA and Israel damaged the Iranian nuclear enrichment plant. The next category is where attack involves the state's critical infrastructure, like atomic weapon control or the nation's electric grid, which, when turned down, can strategically strike the country. Examples of attacks involving critical infrastructure are malware planted by Russia in U.S. electric grid and nuclear plants known as Black Energy and Havex malware. Another example is when Nuclear Power Corporation of India Limited was attacked by foreign state actors, allegedly North Korea. Harmful transgressions can be categorised as proportionate and dealt with less intensity deterrence.

A. Categorising Transgressions into Levels based on the Severity

Using the above-stated severity conditions, we propose a policy to deal with any adverse situation arising from cyber transgression.

1) *Level 1- Cautious Transgression:* Law enforcement handles Level 1 transgressions. Furthermore, states can reach bilateral or multilateral agreements to promote cyber etiquette. An organisation of stature that can regulate cyberspace and promote cooperation can be formed, like Interpol, for practical and quick reprisal and persecution of cyber attackers. Generally, Level 1 transgression involves non-state actors, hacktivists, and other small groups affiliated with the government that are not advanced persistent threats. Cooperation between states can help to enforce punishment for such wrongdoing in the cyber world. Naming and shaming states for not cooperating with cyber offence investigation can always be used to put pressure and deterrence for the future. An example of such cooperative actions is the joint operation for shutting down Silk Road Anonymous Marketplace

by the FBI, Europol etc., shutting down weapons and drugs trading websites, and numerous miscreants were arrested across the globe. Good diplomatic and international relations are the foundation for such collaboration to succeed. Apart from cooperation, good cyber defence capability will serve as a deterrence for small-scale attacks.

2) *Level 2- Heedless Transgression:* Level 2 attacks include both state and non-state actors committing heedless transgressions. And for such transgressions, Metrics for damage should be considered. The economic sanctions against a country and isolation of state on global forums can serve the purpose to some extent, but the use of force such as military surgical strikes can be helpful too. Counterintelligence can be used as deterrence for cyber defence capabilities in Level 2 transgression. An example is the IDF tweet that says, "We thwarted an attempted Hamas cyber offence against Israeli targets. Following our successful cyber-defensive operation, We targeted a building where Hamas cyber operatives work. *HamasCyberHQ.exe* removed.
3) *Level 3- Brazen Transgression:* In the level 3 category, brazen transgression is considered by solid economic sanctions, and international pressure on rogue states using alliances is an effective measure. Level 3 transgressions can result in significant financial loss and fatalities for the state. Military action is always a viable deterrent when dealing with such severe cyber-attacks. However, in the long-run, economic sanctions prove more effective. Terms and conditions for ease of financial sanction are dealt with weightage on the side that has an ethical edge over others. The military operation can bring retaliation of a similar kind by other governments. However, international support is usually towards the country that is more ethical and rationally proportionate in carrying out military action. An example of this is the tussle between Israel and Palestine. A brazen attack was undertaken when Iran defied the international norms regarding nuclear weapons. The USA and Israel dealt jointly to damage the nuclear plant. Iran retaliated with two attacks, one on USA's banks and the other on Saudi Aramco29. Hence Level 3 deterrence must be dealt with maturity.
4) *Level 4- Critical Transgression:* An attack on critical infrastructure and defence systems, including nuclear arsenals, is considered a Level 4 transgression. space infrastructure and electric grids. There have been incidents where states have tried unsuccessful attempts to intrude into such facilities. Havex and Black Energy malware induced by Russia on USA's critical infrastructure are examples of such attempts. A successful attack on such facilities can even trigger a full-scale war between the states.

B. International Efforts for shared responsibility towards damage caused in critical Cyber Infrastructure

In this era of cyber conflict and rapid development in A.I., Attribution will be the biggest unsolved problem in the sphere of cyber-attacks. With the complexity of international relations due to globalisation, the attacks and their response have also increased. Global efforts and collaboration are made to identify the origin of any cyber-attack efficiently. International norms must be updated to include consistent long-term efforts in funding and collaboration in research towards Cyber forensics in the presence of A.I. and other new age technologies. Moreover, the international community should promote an open culture in technological advancements to achieve equality in Cyber Infrastructure. It is essential to classify the complexity of the attack based on Attribution before any action can be taken. Whether the attack can be hunted down to its origin accurately or not is the first question that needs to be addressed.

1) *Scenario I- Attribution is Successful:* Once the adversary's identity is known to the international community, it can be addressed based on the incidents' severity. The New Norm Ladder: The New Norm Ladder is an effort toward mapping norms in international measures across domains (physical, cyber, and economic actions) to the severity of the transgression in the cyber-attack. Attacks with more significant economic damage and fatalities could be met with higher economic sanctions for prolonged periods on the adversary state. Response in terms of cyber and physical force could also be dealt with by rogue states creating havoc in the international community through repeated attacks on critical infrastructures. It is essential for the international community to actively monitor both the interdependence and hostility between states to understand who is most accountable for adopting the norms in the global scenario. The greater a state's capability and will to go against the adversary, the more excellent its accountability to follow the norms of taking action against the adversary.
2) *Scenario II: Attribution is not Successful due to the Increased Complexity of the Attack:* If Attribution fails, shared responsibility can be achieved by taking into account various power indices such as the Military Power Index (MPI), Cyber Power Index (CPI), and so on (CPI), and so on31. Booz Allen Hamilton presented a comprehensive quantitative and qualitative model for Cyber Power. It measured attributes such as Economic and Social Context, Technological Infrastructure, Industry Application, and Legal and Regulatory framework across 19 countries from the G20. However, there is a need to consider states other than the G20 and bring in NGOs and non-state actors into the scenario to come up with a wholesome, reliable index.

C. Cyber Rehabilitation Fund: An effort Irrespective of the Scenario

The international community must establish a cyber-rehabilitation fund to quickly recover the victim state's economy. It can be an effective measure in achieving resilience in terms of support from the international community. Adversary states must pay for the economic damage caused by the attack. In scenarios where Attribution has not been successful, the fund will constitute a contribution based on the different power indices. With such norms in place, the international community will actively participate in forensics investigations and intelligence measures toward finding the adversary state. The international community will be more progressive in sharing technical capabilities and will make active research contributions in forensics and counterintelligence.

VII. CONCLUSION

Retribution might be misapplied when an attack advances more swiftly, thus inviting new players into a broadening conflict. The possibility of a cyber-weapon unintentionally spreading itself through networks into non-targeted states intensifies the danger of unpredictable consequences that can resort to military actions or geopolitical standoffs. In traditional warfare, established norms and conventions provide certainty and slow the manifestation of disasters. Governments could avoid unnecessary use of force if they worked to show transparency, proportionality, and non-proliferation with similar ground rules for cyber warfare. The question remains, is it relevant to base cyber security strategies exclusively on resilience or deterrence? The answer is that Cybersecurity strategies cannot be strictly based on resilience or deterrence. It should be a combination of both. Keeping only one of these as a system base can make a nation's cyberspace entirely defensive or downright aggressive. There should be a balanced effort to improve the resilience and deterrence measures available at one's disposal. Moreover, a nation should use norms to call for international cooperation in actions against the adversary state.

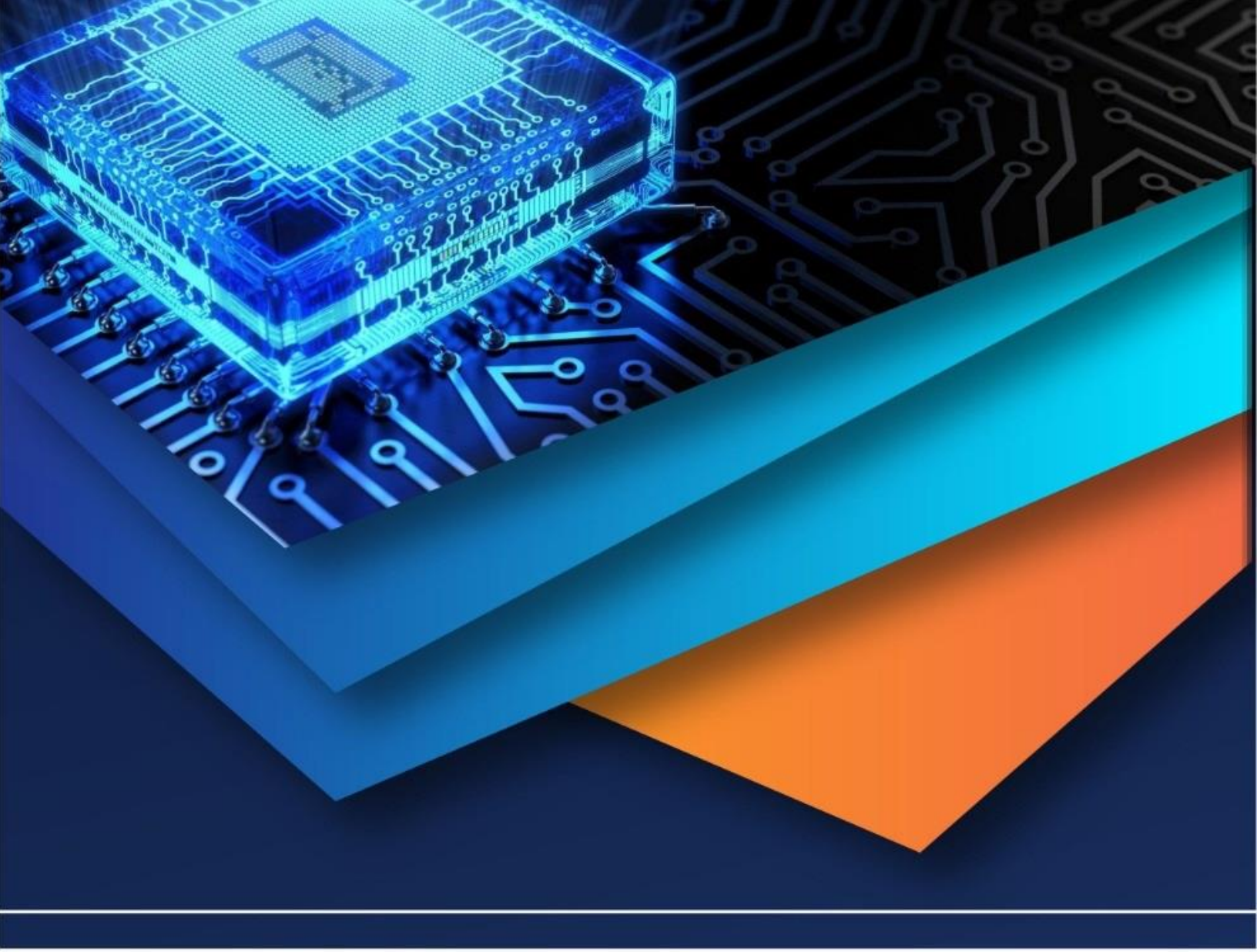
Governments can use the framework to plan a response to any size cyber-attack. It can be a robust framework for achieving deterrence and resilience using Cross-domain. Apart from traditional DIME actions, political tools of Entanglement and normative considerations are used.

This paper also highlights the importance for international organisations to facilitate effective collaboration in pushing the frontiers of research into Forensics and Investigation science to solve the problem of Attribution. The community should also collaborate to review the norms of international action based on levels of transgression and set up a Rehabilitation fund to bring immediate compensation for the loss undergone by the victim state. Also, by forming a tactical cyber retaliation unit, This cyber force, like the United Nations peacekeeping force, can be an effective deterrent method with global cooperation. To protect weaker nations that cannot afford to take any actions on their own. It can avoid a full-fledged war, thus maintaining international peace.

REFERENCES

[1] M. Dogrul, A. Aslan and E. Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," 3rd International Conference on Cyber Conflict, Tallinn, 7-10 June 2011, pp. 1-15
[2] D. Alperovitch, "Towards establishment of cyberspace deterrence strategy," 2011 3rd International Conference on Cyber Conflict, 2011, pp. 1-8.
[3] E. L. Armistead, "Suggestions to measure cyber power and proposed metrics for cyber warfare operations (cyberdeterrence/cyber power)," 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, pp. 1-7, DOI: 10.1109/CYCONUS.2016.7836610
[4] J. Healey and N. Jenkins, "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing," 2019 11th International Conference on Cyber Conflict (CyCon), 2019, pp. 1-20, DOI: 10.23919/CYCON.2019.8756890.
[5] E. B. Kania, "Cyber deterrence in times of cyber anarchy - evaluating the divergences in U.S. and Chinese strategic thinking," 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, pp. 1-17, DOI: 10.1109/CYCONUS.2016.7836619.
[6] S. Alatalu, "NATO's new cyber domain challenge," 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, pp. 1-8, DOI: 10.1109/CYCONUS.2016.7836609.
[7] A. F. Brantly, "The cyber deterrence problem," 2018 10th International Conference on Cyber Conflict (CyCon), 2018, pp. 31-54, DOI: 10.23919/CYCON.2018.8405009.

★★★



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY