BTTN Journal
p-ISSN 2958-1214
e-ISSN 2958-1222

RESEARCH ARTICLE

Assessing Attribution and Credible Deterrence in Cyberspace

Muhammad Imtiaz Sabir [1]

[1] MS scholar at Command and Staff College Quetta, Pakistan.

Article Info

Keywords:

Deterrence, cyberspace, attribution, Cyber Security

Abstract

This study examines the issues that states face in discerning actors within the realm of cyberspace, characterizing these challenges as akin to navigating the unregulated landscape. Lack of an effective attribution mechanism and a credible deterrence framework have significantly contributed to the volatility in cyber domain in contemporary times. This paper argues that states often accuse their adversaries of orchestrating cyber-attacks against them, yet they frequently fail to provide substantial evidence because actors behind attacks in cyberspace leverage the inherent anonymity of cyberspace to evade accountability, complicating the process of attribution even further. In addition, this study also underscores the importance of establishing an effective mechanism of deterrence in cyberspace to dissuade the attacking actors from engaging in malicious cyber activities. In line with this, this paper looks at the cyber space activities through novel perspective of no biasness, without subjectivity and tends to offer the answers of why attribution is problem, is there any possible solution to it in practice. Therefore, this study aims to highlight the ways to attribute the cyber-attacks and highlight the challenges to attribution, especially in the current scenario of states sponsoring indirectly cyber-attacks against many other states by outsourcing their aggressive designs in cyberspace to non-state actors.

[1] Muhammad Imtiaz Sabir is an MS scholar at Command and Staff College Quetta, Pakistan. His research focus is on Security paradigms including deterrence, cyber security and terrorism.

Introduction

Attribution in cyberspace is complex and challenging task. It goes beyond simply finding out an actor responsible for malicious behavior in cyberspace. Harmful cyber activities can take place in numerous ways. Unlike kinetic actions, taken by aggressor, causing more pronounced effects, while having repercussions, which are unfolded over an extended period.[1] However, within the non-cognitive domain, actions may involve compromising a target state's strategic facility, disrupting a major city's grid station, hacking banking system, fomenting unrest in public life by orchestrating social issues. Despite being non-kinetic, the consequences of these actions are extensive and more profound. For example, in 2022, the outcry against the Iranian regime gained momentum following the tragic killing of a woman by morality police in Tehran. This protest received significant backing in cyber domain, leading to widespread demonstrations, while creating a vulnerable situation. External actors seized upon, ultimately disrupting the social life of a nation. [2]

Although cyber criminals employ methods to hide their identity, such as utilizing stolen /fake identities, routing their attacks through various nations /networks. This process can be difficult and complex. For various reasons, such as holding responsible parties accountable, avoiding new attacks, and influencing governmental decisions, it is crucial to be able to precisely attribute cyber-attacks. Developing credible deterrence is also required to deter any potential aggressor from attacking important assets [3] e.g., grid stations, banking systems, causing political instability through

[1] Fiona S. Cunningham, "Accommodative Signaling in Cyberspace and the Role of Risk." *Security Studies* 31, no. 4 (2022): 764-771.

[2] Reuters, *Five killed in Iran during protests over death in custody - rights group*. September 20, 2022. Available at: https://www.reuters.com/world/middle-east/iranian-police-calls-death-mahsa-amini-an-unfortunate-incident-fars-2022-09-19/

[3] Heather Kelly, CNN. 83 Million Facebook accounts are fakes and dupes.https://edition.cnn.com/2012/08/02/tech/social-media/facebook-fakeaccounts/index.html

unrest in public life, government services, national data (NADRA) etc.

Furthermore, problems linked to attribution extend beyond nation-states. While identifying the motives behind cyber-attacks can be challenging, it is not limited to state actors alone; non-state actors solely driven by financial motives also play a significant role. In line with this, this paper looks at the cyber space activities through novel perspective of no biasness, without subjectivity and tends to offer the answers of why attribution is problem, is there any possible solution to it in practice.

Charles L. Glaser[4] and others like Mejia, E. F and Tughral Yamin have discussed various aspects of cyber-attacks while focusing on financial institutions and other critical infrastructure, such as national electric grid.[5] This has further been examined by demonstrating the case of the Japan's attack on Peral Harbor during World War II. The attack was directly attributed to a well-known actor i.e., Japan being the aggressor. However, attacks on financial institutions and other critical infrastructures remained uncertain because of the problem of attribution and appropriate response. Moreover, studies have shed light on effectiveness of deterrence by focusing on employment of all national powers, by doing so states can deter the aggressors for conducting attacks.[6] However, this conception is also ambiguous in cyber domain because of the problem of perfect attribution. Additionally, in the context of Pakistan, scholars have argued that Pakistan places a high priority on security: however in the excessive complex threat environment, cyber security typically falls to the lowest level. There is no denying this truth that ignoring this important reality is only being naïve to visible dangerous situation ahead which will require all out efforts

[4] Charles L. Glaser. Deterrence of Cyber Attacks and U.S. National Security Report GW-CSPRI-2011-5 June 1, 2011.

[5] Tughral Yamin. Cyberspace Management in Pakistan In Governance and Management Review (GMR) Vol.3, No. 1, January-June 2018.

[6] Eric F. Mejia. Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework. Strategic Studies Quarterly, Vol. 8, No. 1 (SPRING 2014).

directed towards cyber space. Pakistan is significantly behind other nations in building a solid cyber infrastructure, unfortunately.

Furthermore, studies have raised question against the effectiveness of Pakistan's cyber security policy and considered that Pakistan is not exempted from cyber-attacks. Deterrence in cyber space is very challenging because countries observes it through the lens of conventional means.[7] This makes the deterrence in cyberspace even more complex. Therefore, this study aims to highlight the ways to attribute the cyber-attacks and highlight the challenges to attribution, especially in the current scenario of states sponsoring indirectly cyber-attacks against many other states by outsourcing their aggressive designs in cyberspace to non-state actors.

Malicious Cyber Activity

Malicious cyber activities is an activity carried out with the intention of harming or damaging computer systems, networks, or digital devices. The attacks that fall under this category may include hadevice misconfiguration, DoS (Denial of Service) attacks, ransomware, and other types of cybercrimes e.g. stealing digital credentials, device misconfiguration etc.[8] Harmful cyber activities can target people, companies, or governments and have a variety of negative effects, including the theft of confidential information, service interruptions, monetary loss, and reputational damage. Cyberbullying, online harassment, cybercrime are also some of the aspects of malicious activities. In line with this, cyber activities has become increasingly crucial in guaranteeing the privacy, security, and dependability of our digital systems and the information they hold as technology continues to advance and become more intertwined with our daily lives.

[7] Akbar Khan, "Deterrence and the Problem of Attribution in Cyberspace: An Analysis of Vulnerabilities and Options for Pakistan." *BTTN Journal* 1, no. 2 (2022): 1-19; Ayaz Hussain Abbasi. Pakistan Needs A Cyber Army To Counter Emerging Risks. The Friday Times January 2022.

[8] Dennis Broeders, Els De Busser, and Patryk Pawlak. "Three tales of attribution in cyberspace: Criminal law, international law and policy debates." *The Hague Program for Cyber Norms Policy Brief* (2020).

Malicious Cyber Activities and its Intent

Cyberspace comprises of a huge amount of information and communication technology (ICT)-based infrastructure that efficiently offers facilities and services for our day-to-day lives. With constant technological developments, cyberspace has made progress in many areas for instance power plants, banking, internet, and other critical infrastructures.[9] This ever-increasing dependence on cyberspace creates a room for malicious cyber activities and give support to actors who are involved in such activities varying from theft of credit card at Point of Sale (PoS) terminals to DoS and attacks on international internet infrastructure. The concentration of such attacks may also differ, as all the attackers have a common objective to disturb the normal day to day activities of the targeted people anonymously.[10] Moreover, regional interests and political motives are also involved in malicious cyber activities. The employment of cyber-attacks by nation-states / other entities to steal trade secrets and sensitive information from their enemies is another typical goal of harmful cyber activity.

To create enhanced cyber security structure, it is crucial to understand the interest behind the harmful cyber activities. There are multiple reasons behind the cyber-attacks, including financial gains, espionage, revenge, hacktivism, personal gains, ideology, etc. Financial gain is one of the main motivations behind cyber-attacks. To acquire financial information, cybercriminals employ a variety of techniques like phishing, hacking, and ransomware attacks. States often employ cybercriminals to collect data on rivals or foreign nations, hack important tools, take revenge and propagate for their personal gains. Mostly, malicious cyber acts are instigated with a very accurate aim against a particular target / entity. For example, in 2013, a super stored was attacked by cyber criminals to hack credit card information of the customers by hacking PoS terminal in the

[9] Hunt R, Zeadally S. Network forensics: an analysis of techniques, tools, and trends. Computer 2012; 45(12):37–43.

[10] Evgeni Moyakine, "Pulling the strings in cyberspace: Legal attribution of cyber operations based on state control." In *Closing the Gap 2022: Responsibility in Cyberspace: Narratives and Practice*, pp. 200-218. Publications Office of the European Union, 2023.

US.[11]However, malicious cyber activities can also be initiated against unknown targets. A survey, jointly carried out by Cyber Security Online (CSO) magazine, Price Water House Coopers, United States Secret Service agency and Computer Emergency Readiness Team, revealed that the biggest motivation of cyber criminals in US was financial gains. Malicious cyber activity from outside the network is also a very common feature in cyberspace; the primary drivers include espionage, monetary gain, and the disruption of the ICT infrastructure. Attribution for all such activities in cyberspace remains enormously difficult. Organizations and governments can only take the necessary precautions to safeguard their networks and data and prevent further assaults by determining the intentions and goals of cyber criminals.

Anonymity in Cyber Space

Anonymity in cyberspace is referred to an individual hiding identity/personal information while using internet. The advantage of being in cyberspace has remained an attraction for cybercriminals as well as state backed actors. Therefore a perpetrator might continue to be shielded from punishment/reprisals for their acts. Any virtual private network (VPN) could be used to conceal one's Internet Protocol (IP) address, a pseudonym/ fake identity can be used to remain anonymous online. Users may profit from anonymity in cyberspace by being able to openly express their thoughts, safeguard their privacy, and stay away from any incident/ harassment.[12] Cyberbullying, online harassment, cybercrime are also some of the aspects of malicious activities. Some platforms and websites have adopted identity verification methods, such as asking users to enter their name, phone number to register an account, to address the drawbacks of anonymity in online. These restrictions, nevertheless, have also come under fire for violating users' right to privacy. In a nutshell, finding a balance between accountability and anonymity in cyberspace is still a challenging problem. While being

[11] BBC 2014, Target data theft affected 70 million customers, for details see, (https://www.bbc.com/news/technology-25681013.

[12] Attribution in Cyberspace: Tecniques and legal Implications:SCN-SI-o88 https://www.researchgate.net/publication/301705275_Attribution_in_cyberspace_techniques_and_legal_implica tions_SCN-SI-088

anonymous an actor can launch an offensive action using a stolen or a fabricated identity. Due to its open architecture, the Internet, a vital part of cyberspace, has expanded substantially. But this feature has also made it possible for people to use false identities and accounts. For example, in 2012, Facebook stated that it had discovered 83 million fabricated Facebook user accounts.[13] Other potential sources of false identities include spoofed IP addresses and bogus email addresses. Domain Name System (DNS) flux, a method that uses haphazardly updating DNS entries, is another way for attackers to conceal their origin. Additionally, there are proxy services that grant access to people, who want to remain anonymous for free and paid for services

Attribution

Any debate of attribution, especially that pertains to law should start by asking why it is that we desire to attribute? It is important to attribute in cyberspace for a number of reasons that include attribution aids in holding people and businesses accountable for their online behavior. To prevent further assaults and advance a safer online environment, it is crucial to find and prosecute cybercriminals. In addition, organizations should be responsible for reporting and raising any cyber related security incident. To comply with these rules and provide law enforcement, attribution is required for the data and prosecute cybercriminals. Moreover, attribution gives important details regarding the strategies, practices, and methodologies employed by cyber criminals. In this context the term "cyber weapon" is notable.[14]

A cyber weapon is a piece of computer code intended to be used for harming physical and cognitive domain of systems, networks and living things.[15] Organizations can utilize such codes

[13] Carr C, Reith M, Gunsch G. An examination of digital forensic models. International Journal of Digital Evidence 2002; 1(3):1–12.

[14] Josh Fruhlinger Stuxnet explained: The first known cyberweapon; Aug 31, 2022. Available at: https://www.csoonline.com/article/562691/stuxnetexplained-the-first-known-cyberweapon.html.

[15] Irani D, Balduzzi M, Balzarotti D, Kirda E, Pu C. Reverse social engineering attacks in online social networks. In Detection of Intrusions and Malware, and Vulnerability Assessment. Springer: Berlin Heidelberg, 2011.

for analyzing the potential threats and its mitigation. Accurate attribution is essential to avoid miscommunications, disputes, and wars. This is crucial in cyberspace, to enable incident response, ensure legal and regulatory compliance, promote accountability, deliver threat intelligence, and uphold positive international relations.

Essentials and Techniques of Attribution

The internet's anonymity makes attribution very difficult. Also, the variety of online activities is intimidating. Attribution is a complicated undertaking that can be comprehended through understanding of the following traits/levels:-

- Level 1, attribution is accomplished when identification of cyber weapon is utilized in cyber-attack.
- Level 2 is achieved when the origin of a place that carried out the cyber-attacks is identified.
- Level 3, entails identifying the actual offender.

Technical attribution is related to level 1, however human attribution or technical attribution both could be related to level 2. Level 3 only has a connection to human attribution. These steps are critical for mounting a calculated counter measure against a known perpetrator.[16] The three stages may not be accomplished because of the challenges with attribution. Generally, an increased degree of attribution can only be acquired when the minimum level is achieved.

In the offline world and in the digital realm, correct attribution is crucial. Few methods of attribution, which are frequently used includes digital forensics, malware based and indirect attribution for enhanced safeguarding, recovering, interpreting, and validating data from digital artefacts as evidence in a criminal investigation. Items which are investigated include

[16] Layton R, Watters P. Indirect Attribution in Cyberspace Handbook of Research on Digital Crime. IGI Global, 2014

computer systems, storage, electronic papers, and database.[17] In addition to the above-mentioned technique, the primary source of malicious activity in cyberspace is malware.[18] A host can be compromised by malicious code through physical access or via a network connection. Due to the challenges of identifying the attacker, the criminal identification, through malware is difficult. Malware-based analysis is typically used to identify the cyber weapon deployed (level 1 of attribution). In certain circumstances, malware-based analysis may also help pinpoint the attacker's location (level 2 attribution), if the signature of previous attacks are recorded.

Indirect attribution refers to assigning responsibility for an attack (or crime) to an attacker (or criminal) based on statistical models of the attacker's behavior. This kind of behavioral models has a variety of characteristics, including coding resemblances, social network analyses, and writing styles. These traits can be combined, which is utilized to create profiles of potential attackers. Both absolute and relative attribution are possible outcomes of indirect attribution. In the first situation, the real offender is found, however in the second, identification is still based on an earlier occurrence.[19] For instance, it can be assumed that one person committed two different types of malicious activities without revealing the attacker. To create criminal profiles, indirect attribution uses methods like genetic algorithms, support vector machines and neural networks. To create detailed profiles of criminals, however, a large amount of data must be provided.

Is Attribution Possible?

It can be difficult and complex to attribute activities in cyberspace, but in rare circumstances, it is possible to identify the people, teams, or organizations behind a cyber-attack. One of the factors that

[17] Hunt R, Zeadally S. Network forensics: an analysis of techniques, tools, and trends. Computer 2012; 45(12): 36–43.
[18] Irani D, Balduzzi M, Balzarotti D, Kirda E, Pu C. Reverse social engineering attacks in online social networks. In Detection of Intrusions and Malware, and Vulnerability Assessment. Springer: Berlin Heidelberg, 2011.
[19] Layton R, Watters P. Indirect Attribution in Cyberspace Handbook of Research on Digital Crime. IGI Global, 2014.

affects the ability to attribute a cyber-attack is the level of sophistication of the attackers, the techniques, used, is to conceal their identities, the quantity and quality of technical data available, and the level of cooperation and information sharing. In exceptional cases, attribution can be made with a high degree of certainty, particularly if the attackers made mistakes or used less sophisticated techniques. For instance, an attacker's digital footprint, such as a specific malware type or a distinctive network signature, might provide crucial information. Even if the perpetrators can be identified, it could be difficult to take legal action against them, especially if they are in a country that would not cooperate. [20] In attribution, sometimes it is possible to pinpoint the culprits, which can be a vital step in thwarting further attacks and enhancing cyber security.

Existing laws Addressing Attribution

Attribution is necessary in an authorized setting for starting criminal investigation, filing a lawsuit, and taking legal action in the form of another cyber incident as retaliation. In both the circumstances, the motivation is either punishment or deterrence. It is crucial for having the right attribution for self-defense. [21] The erroneous attribution of a cybercrime has repercussions. Even, if the appropriate party is targeted for a cybercrime as a reaction, there may still be repercussions.[22] The extent of the effects may also differ i.e., targeting the right adversary without tangible proof may bounce back in the form of legal battle or an adversary with greater cyber offensive potential may direct all its energies to find more vulnerabilities leading to more exploitation. Certain replies, like hack-backs, pose grave dangers to innocent people.

A nation-state may experience various degrees of international hostilities and ramifications because of faulty

[20] Angelyn Flowers, Jawwad Shamsi Attribution in Cyberspace: Techniques and legal Implications: SCN-SI-o88.

[21] Anushka Kaushik. Attribution in Cyberspace: Beyond the "Whodunit". Published in Globsec May 2018.

[22] Ahmad Khan. Addressing Cyber Vulnerabilities through Deterrence. Vol. 11 No. 1 (2022): Journal of Contemporary Studies Vol Xi, No 1, Summer 2022, NDU Islamabad

attribution and response. Because the later affects the former, it is challenging to discuss about the legal elements of attribution. Attribution should not merely be seen as a technological problem; rather, it should also be seen as a policy problem, the solution of which depends on the specific kind of technical problem. The difference focuses on amount of evidence required to link a cyber-action to its alleged perpetrator.[23] Both the government and the commercial sector are faced with the dilemma of how to prevent unwanted malicious cyber incident or a cybercrime.

For instance, was the incident, a malicious cyber incident or a cybercrime? Does the cyber activities put a country's security at risk? Is the victim of the attack, a single individual whose identity has been compromised or any business whose intellectual property has been stolen? The answer to these questions has an impact on attribution level that is necessary to be achieved, along with the type of attribution that is required. The "why" of attribution in domestic legal proceedings depends on who is involved? Private sector organizations are more focused on damage control and prevention whereas law enforcement agencies are worried about attributing it to humans so that they can be prosecuted.[24]

The Convention on Cybercrime of the Council of Europe, specified four types of computer-related offences for which parties must define and sanction security breaches, forgery and fraud, copyright infringement and child pornography. The goal of the cybercrime convention is to encourage the implementation of suitable laws and international cooperation to safeguard society from it. However, many countries around the globe have enacted laws to address domestic cyber related issues to prosecute cybercrimes involving crimes related identity theft, copyright act, abuse act, computer fraud, cyber stalking and cyber bullying. But on the other hand, if any state is involved in cyber related activities, it is often categorized as an event of national security rather than an event of criminal nature. The prevalent approach in such situations

[23] Reith M, Carr C, Gunsch G. An examination of digital forensic models. International Journal of Digital Evidence 2002; 1(3): 1–12.
[24] BBC Report. Target Data Theft affected 7- Million customers.https://www.bbc.com/news/ technology-25681013.

could be compared to hostile cyber event to a war act, enough to be covered by international treaties.[25] The retaliation, is decided with the guidelines according to the law of armed conflict.

The prevention and mitigation of malicious cyber activities is a critical aspect of cyber security. This requires a combination of technical safeguards. For example, intrusion detection systems, firewalls and antivirus software as well as effective policies and procedures, such as user education and incident response plans.

Deterrence in Cyberspace

Nonetheless, deterrence is a critical component of cyber security strategy and can help to reduce the risks of cyber-attacks by dissuading future attackers. Deterrence in cyberspace is the practice of using threats of punishment or vengeance to deter cyber-attacks. However, the existing challenges in cyberspace make deterrence difficult to be achieved. Achieving deterrence in cyberspace depends on accurate attributions towards cyber-attacks. Enhanced technological skills are required for this. This also includes a readiness to cooperate with other nations, organizations and information sharing.

In cyberspace, there are several different types of deterrence, including, i) deterrence by denial that seeks to discourage attackers by making it challenging for them to accomplish their objectives, through robust safety measures. ii) deterrence through punishment, by threatening attackers. This eventually discourages an attacker to conduct any crime.[26] This can entail taking legal action, imposing economic sanctions, or launching an offensive. Deterrence in cyberspace might be challenging to accomplish because it calls for

[25] Boebert W. A survey of challenges in attribution. In US National Academy of Sciences. Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, 2010; 41-54.

[26] Lupovici, Amir. "Deterrence through inflicting costs: Between deterrence by punishment and deterrence by denial." *International Studies Review* 25, no. 3 (2023): viad036.

precise appreciation of attacks and readiness of a coordinated response directed at them. [27]

The deployment of offensive cyber operations by governments to discourage other states from launching cyberattacks is a modern example of deterrence in cyberspace. For instance, according to reports, the US Cyber Command, initiated a cyber-operation against Iranian hackers in 2020 who were thought to be behind attacks on US businesses and infrastructure. This operation was intended to serve as a deterrent, showing other state actors that the US was prepared and willing to use its own offensive capabilities to counter cyber-attacks. The US sought to dissuade future attacks from state-sponsored hacking groups by showcasing its capacity to respond to cyber-attacks in kind.

Problems with Attribution

Attribution is highly critical aspect of an effective deterrence strategy in cyberspace. Secrecy permits harmful cyber actions by state and non-state entities. Security institutions and intelligence community are making efforts for collection of sources, analysis, and the dissemination capabilities of intelligence, attribution, warning, and an assists in reducing signature of involvement by state in cyberspace.[28] The idea that non- state cybercriminals can be used by nation states to attack an adversary so as to hide their involvement in hostile online activity is particularly a difficult challenge in the field of cyber security. It is crucial to investigate the circumstances that would motivate states to employ non-state hackers. There are number of things that can affect this choice. The level of support required to accomplish a particular operational goal, the worth of the state's objective in comparison to the probable consequences of getting caught, and the alignment of the state's and

[27] Borghard, Erica D., and Shawn W. Lonergan. "Deterrence by denial in cyberspace." *Journal of Strategic Studies* 46, no. 3 (2023): 534-569.
[28] Lonergan, Erica D., and Jacquelyn Schneider. "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation." *Journal of Cybersecurity* 9, no. 1 (2023): tyad006.

hacker's goals can all influence the extent of state support for non-state hackers.[29]

Attribution Difficulty

The absence of attribution is caused by a variety of circumstances. Though first level of attribution is accomplished by analysis, a high degree of attribution necessitates acquiring a solid proof followed by strict legal regulations to curb malicious activities online. Following are some of the potential causes which make attribution difficult:-

- **Use of Proxies.** Attackers frequently hide their identities and locations by using proxy servers and anonymizing methods, making it challenging to identify who launched the attack and where they were located.
- **Inadequate Technical Resources**. In addition, lack of technical resources and expertise may prevent law enforcement agencies and security professionals from locating the attacker and tracing the origin of attacks. at
- **Absence of Cyber laws**. Anyone in the world can start a cyberattack, and various nations have distinct cybercrime laws and regulations. Sophisticated technology can make it easier to find out the whereabouts of the attackers, however, this may not be the case with all states.[30] This makes it challenging to trace and bring attackers to justice, especially if they are in a nation that is unwilling to cooperate in information sharing or extraditing suspects.
- **Collaboration Among Different Stakeholders.** At the national level, several groups have a stake in preventing criminal conduct in cyberspace. For example, cooperation among human rights defenders. The government is required to define a privacy infringement while monitoring the

[29] Timothy M. McKenzie Colonel, USAF. Is Cyber Deterrence Possible? CPP–4 Air University Press Air Force Research Institute Maxwell Air Force Base, Alabama, January2017.
[30] William Banks. Cyber Attribution and State Responsibility. Published by the Stockton Centerfor International Law in Volume 97 of 2021.

internet. All the three factors: policy, law and research sectors must cooperate to assess the necessities of attribution and explore ways that how they may be implemented into newly created laws and regulations.[31]

- **Use of Botnets.** Botnets are the networks of compromised computers which are operated distantly by an attacker. They are utilised to launch attacks from numerous areas, making it challenging to exactly locate the attacker's origin.

- **Use of False Flags.** To make it appear as though the attack originated from a different source than the actual attacker, attackers utilise false flags, such as leaving false evidence or exploiting compromised devices.

- **Absence of international treaties**. Many cybercrimes breach transnational boundaries.[32] In other words, state or non-state actors may be to blame for crimes committed across international borders. It is conceivable that this is being driven by geopolitical factors. Cross-border cooperation is required in these circumstances for attribution.[33] Security experts around the globe have a consensus that there is significant misunderstanding between the rival states regarding cyberwarfare capabilities about their adversaries.

Conclusion

It takes a lot of information to put together the difficult process of attribution in cyberattacks. The method and result of attribution in cyberspace are significantly influenced by the political context in which a cyberattack takes place. Security corporations are increasingly exposing their attribution procedures in ways that the public may access and consume. It is a big change in today's world.

[31] Erica and Lonergan. "Deterrence by denial in cyberspace." (2023)
[32] Smith Iii, Frank L. "Integrating deterrence into defence science and technology cooperation." (2023).
[33] Mickelberg K, Pollard N, Schive L. US cybercrime: rising risks, reduced readiness key findings from the 2014 US State of Cybercrime Survey. US Secret Service, National Threat Assessment Center. Pricewaterhousecoopers, 2014.

Making such information available to the general public, easily accessible, and most crucially, comprehensible for a novice, is essential given that cyber-attacks,[34] especially in public discourse, tend to be buried in hype and crisis. With the growing instances of states publicly accusing one another of indirectly financing cyber-attacks, this will also increase trust. Sharing of these technical procedures is now routine, particularly when it comes to very complex attacks that involve multiple nations.

Stronger collective defences are facilitated, message and messenger credibility is increased, and the attribution process itself can be improved by allowing knowledge-sharing, process among the expanding network of IT experts and cyber security firms Technical attribution may be improving, but the growing popularity of using hackers or "proxies" that are either directly or indirectly employed by state actors to conduct cyber-attacks only serves to exacerbate the attribution challenges. The issue of attribution is becoming greatly complicated by motivating non-state hackers and private intermediary actors. In this aspect, publicly linking a state to a cyberattack can serve as a credible deterrence. Furthermore, developing strong cyber infrastructure coupled with comprehensive cyber policies, to avoid being vulnerable in the first place is the need of the hour to accomplish deterrence in cyberspace thus foreclosing the challenges related to attribution.

Though achieving deterrence in cyberspace necessitates a multifaceted strategy that includes strong cyber defence measures, alliances, a range of reaction options, and clear communication. To improve the effectiveness of deterrence in cyberspace, a number of measures can be undertaken. An efficient cyber defence can serve to make a cyberattack more expensive and less appealing to attackers by raising the costs involved. This entails putting in place strong security measures and creating efficient incident response procedures.

[34] Mariarosaria Taddeo. How to deter in Cyberspace. Article published in strategic AnalysisJune-July 2018 Journal of Hybrid CoE.