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. Non-state Actors.

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] such as grid stations, banking systems, causing political instability through

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

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

[3] Heather Kelly, 83 Million Facebook accounts are fakes and dupes, CNN, August 3,2012https://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 Pearl 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", *Governance and Management Review (GMR)*, Vol.3, No. 1, (2018): 46-61.

[6] Eric F. Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework", *Strategic Studies Quarterly*, Vol. 8, No. 1 (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 device 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*, Vol.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 store 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 the Cyber Security Online (CSO) magazine, the Price Water House Coopers, the United States Secret Service agency and the Computer Emergency Readiness Team, revealed that the biggest motivation of cyber criminals in the 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 anonymous

[11] "Target data theft affected 70 million customers," *BBC*, 10 January 2014, https://www.bbc.com/news/technology-25681013

[12] Jawwad A Shamsi, Sherali Zeadally, Fareha Sheikh, and Angelyn Flowers. "Attribution in cyberspace: techniques and legal implications." *Security and Communication Networks*, Vol. 9, No. 15 (2016): 2886-2900.

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]Mark Reith, Clint Carr, Gregg Gunsch, "An examination of digital forensic models". *International Journal of Digital Evidence*, Vol. 1, No. 1 (2002): 1-12

[14] Josh Fruhlinger, Stux,net explained: The first known cyberweapon, *CSO*, Aug 31, 2022. https://www.csoonline.com/article/562691/stuxnetexplained-the-first-known-cyberweapon.html.

[15]. Irani, Danesh, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu, "*Reverse social engineering attacks in online social networks," in Detection of*

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

---

*Intrusions and Malware, and Vulnerability Ass*essment (Berlin Heidelberg: Springer, 2011), 55-74.

[16]Robert Layton, Paul A. Watters. *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,

[17] Ray Hunt and Sherali Zeadally, Network forensics: an analysis of techniques, tools, and trends. *Computer*, Vol. 45. No. 12 (2012):36–43.

[18]. Irani, Danesh, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu, "*Reverse social engineering attacks in online social networks," in Detection of Intrusions and Malware, and Vulnerability As*sessment (Berlin Heidelberg: Springer, 2011), 55-74.

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

or organizations behind a cyber-attack. One of the factors that 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 will be difficult to take legal action against them, especially if they are in a country that may 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". Globsec May 2018.

[22] Ahmad Khan, "Addressing Cyber Vulnerabilities through Deterrence," *Journal of Contemporary Studies*, Vol. 1, No. 1 (2022): 50-68.

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] Mark Reith, Clint Carr, Gregg Gunsch, An examination of digital forensic models. *International Journal of Digital Evidence*, Vol. 1, No. 3 (2002):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] W. Earl Boebert, 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] Amir Lupovici, "Deterrence through inflicting costs: Between deterrence by punishment and deterrence by denial." *International Studies Review*, Vol. 25, No. 3 (2023): 36.

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 Lonergan Shawn W. "Deterrence by denial in cyberspace." *Journal of Strategic Studies* Vol. 46, No. 3 (2023): 534-569.

[28]Erica D Lonergan and Jacquelyn Schneider "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation." *Journal of Cybersecurity*, Vol. 9, No. 1 (2023):1-10.

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.

- **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, 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. Stockton Center for 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*."

[32] Smith Iii, Frank L, "Integrating deterrence into defence science and technology cooperation."

[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," *Strategic Analysis*, June-July 2018.

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

RESEARCH ARTICLE

Drone Warfare and Threshold of the Use of Force

Ahmad Ali [1]

[1] Working as a Researcher at the Strategic Vision Institute, Islamabad.

Article Info

Keywords:

Drones, Warfare, Technology, Threshold, Force

Abstract

The proliferation of drones among both state and non-state actors, as evidenced by their widespread use, signals a shift towards more accessible forms of military engagement. In this context, the paper discusses how drones, as unmanned, remotely operated aircraft, have revolutionized warfare by enabling remote engagement and minimizing personnel risk. Concepts such as risk compensation, the 'body bag syndrome', and the potential for drones to lower the threshold for use of force has also been explored. The precision and long endurance of drones, coupled with their cost-effectiveness, emerge as double-edged swords, enhancing military capabilities while raising questions about the ease of resorting to force. The paper highlights the operational advantages of drones over manned aircraft, including rapid deployment, reduced training requirements, and operational flexibility. This paper also explores the transformative role of drone technology in contemporary military operations and examines the impact of drones on the threshold of use of force in contemporary times. Following the thematic analysis of qualitative sources backed by quantitative data, this paper explores how drones have lowered the threshold for the use of force.

[1] Ahmad Ali is working as a Researcher at the Strategic Vision Institute, Islamabad. He holds a degree in Strategic Studies form National Defence University. He can be Reached at ali921887@gmail.com

Introduction

When technologies interact with social, political, and organizational practices, it creates something new in human affairs. Throughout history, numerous disruptive technologies have been developed for use in warfare, such as gunpowder and the atomic bomb. The impact of disruptive technologies is not always immediately apparent and may represent an evolutionary progression building on other technologies.[1] However, the use of drones in military operations has brought a paradigm shift in modern conflicts. The proliferation of drone technology has revolutionized the way states and non-state actors engage in conflicts. Drones are unmanned aircrafts operated remotely. Use of drones significantly alters our understanding of warfare by introducing a new paradigm of remote engagement, where the risks to personnel are minimised fundamentally transforming the tactics and strategies of military engagements. The convergence of this technology with the post-9/11 security environment has led to a new form of warfare that poses a series of challenges to traditional warfare.[2] Particularly, the use of combat drones has reshaped military tactics, and the future conflicts will see a surge in the employment of drones in a conflict.

However, concerns about the ethical implications of drone warfare have been raised. Arguments against drones use centre on the premise that they could diminish constraints on use for force by reducing risks to soldiers, potentially leading to more frequent or easily initiated conflicts.[3] Furthermore, the use of drones as a strike weapon in a combat zone with no human onboard may increase public support for force.[4] While drones may influence attitudes towards war, their direct impact on initiating conflicts remains uncertain, indicating that multiple elements influence the decision-making process surrounding military engagements. In this paper, the use of force specifically refers to actions that are not legitimate, as use of drones to strike in any other country is a breach of sovereignty. In this context, the paper primarily focuses on highlighting the implications of drones on the threshold of use of force in modern times and assesses future escalation risks. This paper also offers

[1] David Hastings Dunn, "Drones: disembodied aerial warfare and the unarticulated threat" *International Affairs*, Vol. 89, No. 5 (2013): 1237–1246.
[2] Ibid.
[3] James Igoe Walsh and Marcus Schulzke, "The Ethics of Drone Strikes: Does Reducing the Cost of Conflict Encourage War?" (Carlisle, PA: The United States Army War College Press, September 2015).
[4] Ibid.

a thorough insight into the evolving dynamics of drone technology and their role in contemporary warfare.

Evolution of Drone Technology

Drones are remotely piloted systems that remained part of military arsenals since the 20th century.[5] In World War I, the United States experimented with drones for the first time, notably the Sperry Flying Bomb and the Kettering Bug, but these efforts faced technological limitations.[6] During the interwar years, significant developments occurred in radio control technology, leading to the US Army's target drone program.[7] During World War II, the United State Army Air Forces (USAAF) experimented with the use of remotely controlled aircraft, albeit on a trial basis. The project named the Aphrodite program involved converting heavy bombers into radio-controlled aircraft for missions against German targets; however, this project could not be successful and was cancelled in January 1945.[8]

Following the World War II, a shift towards using unmanned aircraft for aerial targets instead of repurposing old, manned aircraft was witnessed. One prominent example is Ryan Firebee, who played an important role in this era and led to significant advancements in drone technology. During the Cold War era, use of drones for intelligence gathering saw a rise. It is important to note that the Ryan 147 Lightning Bug was developed as a significant advancement in reconnaissance capabilities.[9]

The Vietnam War was the first conflict in which drones were used. The Vietnam War saw widespread use of the Ryan 147 Lightning Bug.[10] These drones played multiple roles, including reconnaissance,

---

[5] James J. Wirtz, "Drone: remote control warfare," *Intelligence and National Security*, Vol. 34, No. 3 (2019): 456-461.

[6] Dennis Larm, "History and Background," in *Expendable Remotely Piloted Vehicles for Strategic Offensive Airpower Roles* (Air University Press, 1996), 9-24, http://www.jstor.org/stable/resrep13923.

[7] Richard M. Clark, "Evolution of Uninhabited Combat Aerial Vehicles (UCAV)," in *Uninhabited Combat Aerial Vehicles: Airpower by the People, For the People, But Not with the People* (Air University Press, 2000): 9, https://www.jstor.org/stable/pdf/resrep13976.7.pdf?refreqid=fastlydefault%3Af2becbb63702af89cde658d553c2cfdb&ab_segments=&origin=&initiator=&acceptTC=1.

[8] Ibid.

[9] Ibid.

[10] David Axe, "Inside Vietnam's Forgotten Drone War," Daily Beast, September, 27, 2021, https://www.thedailybeast.com/inside-vietnams-forgotten-drone-war

electronic warfare, and propaganda dissemination.[11] Also, in the 1960s, the US tried to develop Stealth drone named Ryan 154 Compass Arrow. It was designed to conduct deep reconnaissance missions over China and was capable of flying at nearly fifteen miles high and capturing ground details as small as one foot. It was designed for long-range, high-altitude reconnaissance; however, the US-China relations improved during this period due to which the development of Ryan 154 Compass Arrow was not considered necessary anymore.[12] However, the technological advancements made during this project contributed to the designs of future stealth fighters, bombers, and drones.[13]

By 1985, the US, inspired by Israel's successful drone program, significantly enhanced its drone production. The RQ2 Pioneer Drone, a collaboration between the US and Israel, emerged in 1986 as a pivotal drone.[14] It is important to note that, this upgraded drone played a significant role during the Gulf War. A decade after this, the development of the Predator Drone in 1996 marked a significant evolution in drone capabilities, introducing weaponized drones to warfare. Drone market is projected to reach $92 billion by 2030.[15]

Role of Drones in Contemporary Warfare

Drones have emerged as an important military platform in modern times, leading to a shift in military tactics. Given that drones offer a quick and cost-effective alternative to military action, the need for large-scale military intervention has decreased. The use of drones in targeted strikes, surveillance, and Kamikaze style attacks are prominent examples of their role in modern times. Effectiveness of drones in the second Nagorno-Karabakh conflict has initiated a debate about whether drones are merely an addition to existing weapon systems, or it is a revolutionary shift. Although, usage of drones in this conflict was one sided i.e., Azerbaijan. However, unmanned aircrafts played a prominent role in countering Armenian ground forces on the battlefield highlighting the vulnerability

[11] Megan, "When Were Military Drones First Used," *Drone Survey Services*, accessed December 17, 2023, https://dronesurveyservices.com/when-were-military-drones-first-used/
[12] "AQM-91 Firefly / Compass Arrow," *Global Security*, accessed December 18, 2023, https://www.globalsecurity.org/intell/systems/compass_arrow.htm
[13] Ibid.
[14] David Daly, "A Not-So-Short History of Unmanned Aerial Vehicles (UAV)," *CONSORTIQ*, accessed December 18, 2023,https://consortiq.com/uas-resources/short-history-unmanned-aerial-vehicles-uavs
[15] Ibid.

of conventional military equipment to drones. Utilization of drones by Azerbaijan played a significant role in determining the outcome of the war. The war concluded with Armenia accepting a ceasefire agreement under severe terms.[16]

In addition, the growing use of Kamikaze or suicide drones in recent times have demonstrated a clear shift towards increasingly disruptive means of engagement. The Nagorno-Karabakh and the ongoing Russia-Ukraine conflicts are important examples of this trend. In the context of Russia-Ukraine conflict, drone models like the AeroVironment Switchblade, the Phoenix, and Zala Lancet-3 have been prominent due to their cost-effectiveness along with their ability to evade conventional air defences.[17] Considering this, it can be argued that drones due to the effectiveness have become an important weapons platform for major military powers. Moreover, drones also have revolutionized Intelligence, Surveillance, and Reconnaissance (ISR) operations. This can be seen from Ukraine's deployment of over six thousand ISR drones against Russian troops.[18] This is because drones provide direct situational awareness of the battlefield leading to precise military strikes on the enemy positions.[19]

Apart from this, drones are also being utilized for broader information warfare. In contemporary times, drones provide aerial documentation of conflict zones that were previously unimaginable. This footage, when disseminated through the media, it influences public opinion. In this context, the Russia-Ukraine conflict is the best example, where Ukraine released drone footage that showed destruction of Russian tanks. This footage was circulated around the world through media contributing to broader information warfare while gathering support from public. Considering this, one could argue that real-time drone footage

[16] Robyn Dixon, "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh and showed future of warfare," *The Washington Post*, November 11, 2020, https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijanaremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html

[17] Aamna Rafiq, "Drone Warfare in Contemporary Conflicts: Five Lessons to Gen Up," (Institute of Strategic Studies Islamabad (ISSI), September 19, 2022), https://issi.org.pk/wp-content/uploads/2022/09/IB_Aamna_Sept_19_2022.pdf

[18] Shaza Arif, "Ukraine and Use of Commercial Drones on the Battlefield*,"* (Center for Aerospace & Security Studies (CASS), June 3, 2022), https://casstt.com/ukraine-and-use-of-commercial-drones-on-the-battlefield/

[19] "Drones in Ukraine and beyond: Everything you need to know," (European Council on Foreign Relations (ECFR, August 11, 2023), https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/

from conflict zones has emerged as a crucial tool for shaping public perception.

Cost Considerations: Are Drones a Financially Viable Option?

It is important to consider financial aspects while analysing the relationship between drones and the employment of force. It is pertinent to note that drones are relatively less costly and are easier to maintain as compared to traditional aircraft.Keeping this in view, drones present a significant advantage when employing force. The financial aspect is particularly crucial when considering attacks against well-defended targets that were previously - too risky for a manned aircraft.

It is crucial to highlight that drones as compared to manned aircrafts are cheaper to manufacture and maintain.[20] This cost-effectiveness is due to their relatively smaller size, simpler design and absence of life support systems for pilot. Furthermore, many components of drones are mass-produced for different commercial applications that further reduce the production cost. For instance, the Houthis launched multiple domestically produced suicide drones towards allegedly Israeli-linked commercial vessels[21] and cost of each drone is around $2000.[22] However, the cost of munitions to counter these drones range from $1 million to $4.3 million per unit.[23] This highlights that the countermeasures for drones are far more costly than a suicide drone itself.

Apart from this, the comparison of a Reaper drone with F-35 Lightening II further highlights the cost-effectiveness of drones. A Reaper drone requires the support of two pilots, a ground control station, and a secure data link for communication and control. With these requirements, the operational cost of a Reaper drone for flight of an hour is around $3250.[24] It is important to note here that each Reaper drone

[20] Richard J. Gross, "Military Drone Cost: Breaking Down the Price Tag (2023)," Propel, July 17, 2023, https://www.propelrc.com/military-drone-cost/
[21] "High Costs of Countering Drones Alarm Pentagon," *Dawn*, December 24, 2023, https://www.dawn.com/news/1800350/high-costs-of-countering-drones-alarmpentagon
[22] Ibid.
[23] Ibid.
[24] Wayne McLean, "Drones are cheap, soldiers are not: a cost-benefit analysis of war," *The Conversation*, June 26, 2014,https://theconversation.com/drones-are-cheap-soldiers-are-not-a-cost-benefit-analysis-of-war-27924

costs around $32 million.[25] On the other hand, the initial cost of purchasing F-35 Lightning II is over $109 million.[26] When it comes to the annual operational expenses, this aircraft stands at $5 million.[27] Similarly, the cost for each hour of flight is estimated to be $44,000.[28] To simply put, the US Department of Defense (DOD) has projected that the total cost for purchasing, operating, and maintaining single F-35 Lightning II aircraft and its associated systems for its entire life to be nearly $1.7 trillion.[29] This comparison between an advanced aircraft and a combat drone highlights a significant difference in purchasing and maintaining them. Similarly, comparison between the fourth-generation aircrafts and less sophisticated drones show that drones are cost effective.

Do Drones Encourage Use of Force?

It is argued that drones lower the threshold for use of force. The key argument is that drones enable countries to carry out attacks without any risk of casualties to its own personnel resulting in willingness to engage in drone attacks even in situations where it would not otherwise use military force. Drones, by their nature, have the potential to encourage states to engage and use force even in situations where diplomatic means could have resolved the issue.[30] Apart from the already discussed arguments, further discussion surrounding drones and threshold of use of force are deliberated below.

---

[25] "MQ-9 Reaper: All about the US drone that crashed into the Black Sea," *The Economic Times*, March 16, 2023,https://economictimes.indiatimes.com/news/international/us/mq-9-reaper-all-about-the-us-drone-that-crashed-into-theblacksea/articleshow/98645377.cms?from=mdr

[26] Justin Hayward, "How Much Does An F-35 Cost?" *Simple Flying*, December 20, 2023, https://simpleflying.com/how-much-does-an-f-35cost/#:~:text=The%20F%2D35%20Lightning%20II,to%20%24109%20million%20per%20aircraft.

[27] Wayne McLean, "Drones are cheap, soldiers are not: a cost-benefit analysis of war," *The Conversation*, June 26, 2014,https://theconversation.com/drones-are-cheap-soldiers-are-not-a-cost-benefit-analysis-of-war-27924

[28] Marcin Frąckiewicz, "How much does an F-35 cost per flight hour?" *TS2*, November 4, 2023, https://ts2.space/en/how-much-does-an-f-35-cost-per-flight-hour/#gsc.tab=0

[29] United States Government Accountability Office, *F-35 Joint Strike Fighter: More Actions Needed to Explain Cost Growth and Support Engine Modernization Decision*, May 30, 2023,https://www.gao.gov/products/gao-23-106047#:~:text=The%20F%2D35%20Lightning%20II,options%20for%20modernizing%20its%20engine.

[30] Marcus Schulzke and James Igoe Walsh, "Drones and Moral Hazard," in *Drones and Support for the Use of Force* (University of Michigan Press, 2018), pp. 105-128, https://muse.jhu.edu/pub/166/oa_monograph/chapter/2234205#:~:text=Because%20drones%20permit%20force%20to,states%20Page%204%20Drones%20and

Risk Compensation

The concept of risk compensation suggests that when there is a constant level of acceptable risk, decreasing the risk associated with a certain action can increase its acceptance.[31] In other words, if something becomes safer to do then people may do it more frequently. Drones reduce the direct human costs of conflict for the side using them. As a result, risk is transferred from the party employing them to the party against which they are being utilized. This leads to an increased risk-taking by those protected from the immediate consequences of their actions. In the context of drone warfare, the idea of risk compensation comes into play when there is a shift in how risk is perceived leading to a higher degree of willingness to use military force. This becomes more relevant when targeting areas where risk is high and manned mission could be dangerous. The use of drones in such scenario ensures that even if a drone is lost, there are no direct human casualties on the side of the attacking force leading to a more aggressive action.

In the context of drone warfare, the inclination for military action because of reduction in risks is the core of risk compensation. Apart from this, drones can change risk perceptions in ways that might encourage riskier behaviour. This phenomenon is known as the Peltzman effect.[32] An example that further elucidates this concept is the enhancement of vehicle safety features. These improvements make drivers feel more secure, which may lead to more reckless driving, potentially negating the safety gains. Similarly, in case of drone warfare, the increased sense of security could lead to more aggressive actions, potentially undermining the very goals of reducing casualties and collateral damage. Furthermore, drones can encourage decision-makers to authorise actions that are morally questionable creating a "Moral Hazard". This concept describes a situation where an entity is more inclined to take risks due to the perceived low consequences of failure.[33]

---

[31] Mikkel Vedby Rasmussen, "The Revolution in Military Affairs and the Boomerang Effect," *DIIS Report* 2004:6, p. 9 (Danish Institute for International Studies, 2004), https://www.files.ethz.ch/isn/19255/Revolution_Military_Affairs.pdf

[32] Marcus Schulzke and James Igoe Walsh, "Drones and Moral Hazard," in *Drones and Support for the Use of Force* (University of Michigan Press, 2018), 116, https://library.oapen.org/bitstream/id/dbc17a3f-949f-4f0a-8b59 accbb273e97c/1004146.pdf

[33] John Kaag and Sarah Kreps, "The Moral Hazard of Drones," The New York Times, July 22, 2012,https://archive.nytimes.com/opinionator.blogs.nytimes.com/2012/07/22/the-moral-hazard-of-drones/

Body Bag Syndrome

Body Bag Syndrome takes on a unique dimension of human psychology. Drones significantly reduce the risk of casualties among militaries, particularly for the side using them, due to the absence of humans on board. This aspect aligns with the public's growing aversion to war casualties, as exemplified by the concept of "body bag syndrome."[34] In traditional combat, the fear of military casualties often influences public opinion and political, leading to a hesitancy to engage in military operations.[35] However, drones tend to minimise the risk to soldiers, thus altering the public and political perception and willingness regarding the use of force. The debate regarding body bag syndrome raises critical questions about drones that lower the threshold for the use of force in international arena. Drone operations' safety leads to increased employment without adequate consideration of moral responsibility.

Precision

One of the key arguments in favour of drone use is their capability to precisely engage targets. The precision of drones increases the likelihood of success while at the same time reducing the human and financial costs. Although it aligns with the imperative to protect non-combatants in conflict zones which is the foundation of International Humanitarian Law (IHL), this precision along with reduced risk and lowered cost presents a scenario that is viewed as advantageous. Consequently, drones are viewed as a preferred method of engagement over other forms of military action leading to lowered threshold of use of force. Therefore, the use of drones raises important questions regarding the threshold for engaging in military action.

Acceptance of Use of Drones

When it comes to the acceptance of drones' usage, targeted countries might perceive drone attacks differently than they would for a manned aircraft incursion. Unlike fighter jets, the absence of human presence in drones can lead to a perception of a less direct form of aggression. This could potentially trigger a different and mild response from the attacked

[34] Philip Everts, "When the Going Gets Rough: Does the Public Support the Use of Military Force?" *World* Affairs, Vol. 162, No. 3 (2000):91–107,https://www.jstor.org/stable/20672578#

[35] Allyson L. Mitchell, "My Neighbor Is A Terrorist: Peacebuilding, Drones, and America's Presence in Yemen," *Beyond Intractability*, November 2012, https://www.beyondintractability.org/reflection/mitchell-neighbor

country compared to a manned aircraft strike. Another reason is that use of drones in the media are portrayed differently than traditional military operations. It is observed that use of force using drones often receive less media coverage compared to ground operations or manned aircraft attacks.[36]

Furthermore, drones' usage has a certain degree of normalisation in the public consciousness due to the increased use of drones in contemporary times. This makes drone attacks seem more routine and less shocking than other forms of military engagement leading to mild reaction. The perception of drone strikes as less aggressive likely triggers a mild response leading to reduced escalation. The targeted country may protest diplomatically; however, the perceived lower level of aggression might not trigger a military response.

Long Endurance

Drones possess the capability to hover over a target area for extended periods unlike manned aircrafts. This endurance allows them to wait for suitable moment to strike. This aspect of drones i.e., ability to loiter enhances the precision of military operations that incentivizes the use of force. Drones are also capable of conducting longer and uninterrupted missions that allows them to cover larger areas for extended durations and engage where needed. The long-endurance drones can operate for over 30 hours without needing to refuel.[37] Keeping this in view, future technological advancements might further enhance this capability, potentially eliminating the need for these systems to land, except for routine maintenance.

Operational Advantages over Manned Aircrafts

Drones offer several advantages in terms of deployment and operationalisation.[38] In this context, drones can be deployed more rapidly

[36] Joanna Frew, "In the Frame: UK Media Coverage of Drone Targeted Killing," *Drone Wars UK*, January 2020,https://dronewars.net/wp-content/uploads/2020/01/InTheFrame-Web.pdf

[37] Thomas G. Mahnken, Travis Sharp, and Grace B. Kim, "Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition," Center for Strategic and Budgetary Assessments (CSBA),2020,https://csbaonline.org/uploads/documents/CSBA8209_(Deterrence_by_Detection_Report)_FINAL.pdf

[38] "The Impact of Drones on Future of Military Warfare," Zena Drone, Accessed January 1, 2024, https://www.zenadrone.com/drones-impact-the-future-of-military-warfare/

and with greater ease. This speed in deployment is a significant advantage in scenarios that require immediate military action. Also, operating drones requires less extensive training compared to flying conventional aircraft. Drones like Mojave allows forward-basing operations without relying on traditional paved runways or extensive infrastructure.[39] Its ability to take off and land from a remote surface significantly enhances operational flexibility. Combination of factors such as rapid deployment, less extensive training requirements, and independence from runways, significantly lower the threshold for the use of force. Their ability to be operated from almost anywhere makes them a preferred choice for a range of military actions. As a result, the decision to employ military force becomes easier and more feasible.

Use of Drones by States

The debate until now suggests that drone technology has reduced the threshold for use of force in contemporary times. Moving forward, analysing various international incidents involving drones provides ample evidence for the debate regarding drones and how they lower the threshold of use of force. These events not only portray the decreased risk of human casualties but also underscore other aspects, such as cost efficiency and the evolving nature of military engagement. The US military actively employs drones in combat, using them for both surveillance and offensive operations[40]. To start with, the US military has been utilising drones for decades. Many scholars have comprehensively explored the public's perception of use of military drone within the framework of American foreign policy. In the US, the use of drones in military operations garners significantly more public support than ground operations, a preference that transcends political affiliations, suggesting a bipartisan consensus in favor of drone use.[41] However, in contemporary times, other states and even non-state actors are utilizing drones in

[39] "General Atomics Aeronautical, General Atomics Aeronautical Systems Inc, Accessed January 1, 2024, https://www.ga-asi.com/remotely-pilotedaircraft/mojave

[40] Christopher Woody and Jake Epstein, "Russia and Ukraine are Fighting the Kind of Drone War the US Military Has Been Worrying About, and It's Scrambling to Prepare for a Future That's Already Here," Business Insider, September 1, 2023, https://www.businessinsider.com/russia-ukraine-fighting-drone-war-us-military-was-waiting-for2023-8

[41] James Igoe Walsh and Marcus Schulzke, "Introduction," in *Drones and Support for the Use of Force* (University of Michigan Press, 2018), 1-28, https://www.jstor.org/stable/j.ctvh4zhx8

combat and drones have lowered the threshold for use of force due to multiple factors discussed previously.

One prominent example of this is that allegedly Israel conducted a drone strike in Iran that targeted a military factory near Isfahan, in January 2023. This is one instance that shows how drone technology has lowered the threshold for military engagements, allowing states to conduct precise operations like this with reduced risk.[42] By opting for a drone strike, Israel demonstrated the ability to target key facilities in Iran while minimizing the potential for direct confrontation and the risks typically associated with traditional military actions. In the second case scenario, Russia in April 2008 downed a Georgian Hermes 450 drone.[43] Eventually the countries fought a war in August that year; however, the war could have started months ago if Russia had shot down a manned aircraft instead. These incidents underscored how drones have made it more feasible for countries to respond to perceived threats with less regard for the traditional consequences associated with manned aircraft engagements, primarily due to the lower financial and human costs involved.

Apart from this, Israel downed an Iranian armed drone in February 2018 which demonstrates lowered threshold for engaging in provocative actions.[44] In this case, Iran sending a drone with explosives was a proactive action. In response, Israel downed this drone and further escalation did not take place. This incident suggests that drones do lower the threshold of the use of force. This particular incident shows a shift towards more frequent and bold military actions, fuelled by acceptability of use of force by utilizing drones. Another incident took place in June 2019 when Iran downed a US Global Hawk in the Gulf of Oman.[45] People

[42] Dov Lieber, Benoit Faucon, and Aresu Eqbali, "Israel Drone Strike Hit Iranian Weapons Facility," *The Wall Street Journal*, January 30, 2023, https://www.wsj.com/articles/israel-drone-strike-hit-iranian-weapons-facility-11675110298

[43] Seth Frantzman, "Remember when a Russian MiG-29 shot down a Georgian drone?" Drone Wars, July 8, 2020, https://dronewars2021.com/2020/07/08/remember-when-a-russian-mig-29-shot-down-a-georgian-drone/

[44] "Israel Says Iranian Drone It Shot Down in February Was Carrying Explosives," *Reuters*, April 14, 2018, https://www.reuters.com/article/us-israel-iran-drone/israel-says-iranian-drone-it-shot-down-in-february-was-carrying-explosives-idUSKBN1HK2LU/

[45] Joshua Berlinger, Mohammed Tawfeeq, Barbara Starr, Shirzad Bozorgmehr, and Frederik Pleitgen, "Iran Shoots Down US Drone Aircraft, Raising Tensions Further in Strait of Hormuz," *CNN*, June 20, 2019, https://edition.cnn.com/2019/06/20/middleeast/iran-drone-claim-hnk-intl/index.html

perceive drones as a less provocative option than manned aircraft, enabling a response that might otherwise be considered too escalatory or risky. If we had downed a manned aircraft instead of a drone in this scenario, the dynamics would have been different. Similarly, in the Russia-Ukraine Conflict, both sides are prioritising drones to strike each other's facilities and opting not to deploy their substantial fleets of manned aircrafts.[46] This choice stems from the significant risks posed by both sides' surface-to-air missiles that endanger pilots supporting ground operations. Consequently, Moscow and Kyiv have engaged in a less costly form of warfare through drones. This shift highlights that even in active conflicts, the adoption of drones has effectively lowered the threshold for the use of force.

In all these instances, escalation dynamics may have been more likely to spiral into armed conflict if manned aircrafts would have been used instead of drones. Collectively, these incidents reinforce that drone technology in military operations has indeed lowered the threshold for the use of force. A shift characterized not only by the reduced risks and consequences, but also by the more cost-effective nature of drones compared to manned aircraft operations. These factors have led to an increased tendency for states and non-state actors to engage in military actions leading to alteration in the dynamics of international conflict.

Impact on Threshold of Use of Force

Drones have brought a transformation in how militaries engage in conflicts.[47] The wide range of availability and capabilities of drones have led to lowering the threshold of use of force. This is because countries and even non-state actors find drones an attractive platform in peacetime as well as during conflict. Additionally, technological advancements particularly drones create a scenario where political leaders might no longer feel the need to seek public approval or consensus before engaging in warfare or using force. This is due to the perceived reduction in risk to their own soldiers potentially making the decision to go to war easier.[48]

[46] "Why hasn't Russia mobilised its vast air power against Ukraine?" *Al Jazeera*, March 2, 2022, https://www.aljazeera.com/news/2022/3/2/why-hasnt-russia-mobilised-its-vast-air-power-against-ukraine

[47] Sarah Kreps and Micah Zenko, "The Next Drone Wars: Preparing for Proliferation," *Foreign Affairs,* Vol. 93, No. 2 (2014): 68–79.

[48] Marcus Schulzke and James Igoe Walsh, "Drones, Casualties, and Attitudes," in *Drones and Support for the Use of Force* (University of Michigan Press, 2018), 62.

Drones and Future Escalation Risks

The "second drone age" is marked by the widespread use of military drones and armed commercial drones signalling a turning point in drone warfare.[49] In this era, both state and non-state actors are increasingly vying for aerial dominance in and beyond traditional conflict zones. During the first drone age, the US held a monopoly on military drones using this technology predominantly in uncontested airspace. Operated by the US military, the Central Intelligence Agency (CIA), and the militaries of certain allies, these drones were primarily employed to target and eliminate individuals labelled as terrorists and insurgents, both within and beyond established conflict zones.

In the second drone age, various states are increasingly utilizing military drones, offering an easy way to carry out lethal strikes from the skies. The number of countries with these technologies has risen sharply from 60 in 2010[50] to 102[51] in 2019, a 70% increase. Among these, about 40 states, including Israel, Iran, the UK, the US, Turkey, France, the UAE, Saudi Arabia, Egypt, Nigeria, and Pakistan, are equipped or acquiring large drones capable of deadly attacks.[52] These states have used drones in operations or close air support. Currently, there are 21,000 confirmed unmanned aircraft in operation globally, but the actual number is probably higher than 30,000.[53] For instance, during the 2020 Azerbaijan-Armenia conflict over Nagorno-Karabakh, both sides actively used and shot down each other's drones. Military drones are used globally in diverse operations such as counterterrorism,

[49] James Rogers, "Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age," in *A Comprehensive Approach to Countering Unmanned Aircraft Systems* (Joint Air Power Competence Centre, January 2021), https://www.japcc.org/chapters/c-uas-future-threats-military-uas-terrorist-drones-and-the-dangers-of-the-second-drone-age/

[50] Dan Gettinger, *The Drone Databook* (The Center for the Study of the Drone at Bard College, 2019), IX, https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf

[51] James Rogers, "Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age," in *A Comprehensive Approach to Countering Unmanned Aircraft Systems* (Joint Air Power Competence Centre, January 2021), https://www.japcc.org/chapters/c-uas-future-threats-military-uas-terrorist-drones-and-the-dangers-of-the-second-drone-age/

[52] Ibid.

[53] Dan Gettinger, *The Drone Databook* (The Center for the Study of the Drone at Bard College, 2019), IX, https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf

counterinsurgency, peacekeeping, border control, anti-piracy, drug interdiction, anti-smuggling efforts, firefighting, and environmental conservation. However, it is important to note that since the 1980s, at least 28 countries have operated drones beyond their national boundaries.[54] Opting for military drones as a low-cost, seemingly low-risk solution is becoming more common. However, even precise drone strikes have broader political ramifications and unintended consequences, potentially escalating conflicts or igniting new hostilities.

Conclusion

In a nutshell, drones have significantly altered the way, modern military engage leading to a lowered threshold for the use of force. The ability of drones to carry out precision strikes along with kamikaze attacks with minimal risk to personnel coupled with their cost efficiency and long endurance has altered military calculations. This shift is evident in the use of drones in situations where the risk for manned aircraft was too high. The risk compensation phenomenon and the body bag syndrome further clarify the relationship between drones and the use of force. Drones present an attractive option for military action considering reduced risk to military personnel. Additionally, the logistical advantages of deploying drones further lower barriers for military action. Apart from this, drones have certain degree of acceptance in the society and media has normalised their usage leading to a mild response from the country attacked. This scenario further incentivises the drone usage instead of manned aircrafts. This transformation raises critical questions about the long-term implications for international security. All the debate suggests that the drones have lowered the threshold of use of force

[54] Ibid, XII.