INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

IS INFORMATION SAFE ONLINE? CYBER MERCENARISM, AN EMERGING THREAT LANDSCAPE.

AUTHORED BY - VAHINI. PARAMESWARAN
& NANDINI RAO BUDHAGAVI

Abstract

As Robert Mueller accentuated "There are only two types of companies: those that have been hacked and those that will be." Security and Privacy constitute what is called as a "Data Breach." There is a rise in the graph of cyber threats from data stealing to information leakage with a parallel increase in the lack of ability to identify and protect from these threats. Prior to any awareness of the user, the attackers identify the system vulnerabilities and exploit it for malicious reasons. The breach of security and privacy at individual, group, organisation, and societal level shows the extent of threat information possesses.

The development of cyber mercenaries in recent years has posed a huge cybersecurity threat in India, with far-reaching ramifications for the country. These cyber mercenaries are essentially private entities or individuals with advanced hacking skills who can be hired by nation-states, criminal organizations, or even competing enterprises to perform cyber-attacks for a variety of reasons. In India, the influence of cyber mercenaries has been diverse. They attacked key infrastructure, government organizations, and private businesses, resulting in data breaches, financial losses, and service interruptions. This not only jeopardizes India's national security, but also its economic stability and technological progress. With the distortion, mutilation, and the threat of identity theft by Mercenarism, can it be concluded that no information that is connected to the internet is unhackable and that information security is not concrete? Further, the research attempts to answer the gap relating to the involvement of non-state actors.

Keywords: cyber mercenary, state actors, non-state actors, military

ISSN: 2582-6433

Introduction

Cyber space, a growing geopolitical arena that has resulted in as an emerging threat. An incipient growth of Internet has made information sharing easily operatable and accessible, depicting an emergent threat in economic and social harm. Entry into the network or computer systems due to low barriers allows influence of adversaries which was in precedence a power possessed by the government. A lost state control over cyber weapons or intermediaries, privatization of cyber offences has given rise to a major problem of attributing accountability and liability of the attacks. One such criminal actors engaging in activities for any country is cyber mercenary Not an undefined term rather a term that has multiple layers to it, that disables forming of a concrete definition. " A cyber mercenary can be defined as an individual or group of experts who can offer their skills to anyone who will pay them a good amount of money.[1]

A criminal actor engaging in activities for any country. The use of third parties or proxies has been found all through history. The states use third parties to exploit and achieve their political objective. A wide access to internet services within the primary, secondary and the tertiary sector has caused a shift to the digital world incentivising exploitation of the cyberspace by both the state and non-state actors. There is an immense risk of security as acute vulnerabilities cause the system fall prey to cyber-attacks as various sectors, organisations and government rely on services like pensions, payroll, and healthcare. The rise in "hire-for-fire" firms based in countries all across. These firms are identified and hired by governments, global clients, and departments that that targeted healthcare, legal and individuals. [2]

Review of Literature

In the article titled, "*Cyber Mercenaries: A new weapon in International Conflict",* the author outlines the paper in two-fold manner, firstly by the introduction of the term cyber mercenaries, the legal challenges it raises, and several examples from the real world to show their credibility. The second part of the paper will touch upon the possible impacts of cyber-attacks conducted by cyber mercenaries on international relations nowadays. The paper restricts itself to limited literature review and scope in its research. It just highlights the challenges but does not address

[1] Tim Maurer, cyber mercenaries: the state, hackers, and power
[2] da Cruz, José de Arimathea and Pedron, Stephanie () "Cyber Mercenaries: A New Threat to National Security," International Social Science Review: Vol. 96 : Issue. 2 , Article 3.

ISSN: 2582-6433

the source of such a problem. (Michael Andruch-, 2021)[3]

In the paper titled *"Rise of Cyber Mercenaries*," Ataa Dabour talks about state-sponsored cyber mercenaries and the dangers behind such cybersecurity threat. Gap in this research is that it only concerns itself with the state-sponsored mercenaries and does not scrutinize private entities involved.(Ataa Dabour, 2021)[4]

As stated by the author in *"Information privacy concern at individual, group, organization and societal level,"* Analysis of different studies of privacy concerns related to information arising because of application that are based on computer-based information system at different levels i.e., individual, group, organisational and societal levels. In- Depth analysis of the influencing factors that affect the privacy and the association of various application and domain with privacy concerns such health care, banking, e-commerce, e-business, internet, cloud computing, social networking, governance etc to mention a few. Increase in CBIS at micro and macro levels to process, store, share information. But it brought with it two major concerns privacy and security. (Dillip Kumar Rath and Ajit Kumar,2020)[5]

In the working group report use of cyber mercenaries is means of violating humans right and impeding the rights of people to self-determination. The Working group identified it as contemporary category of actors that are engaged in mercenary activities. The existence of commercially accessible disruption, interference with the deterioration or destruction of computer systems or networks, and information exfiltration is a danger to cyberspace's safety and stability. Tools used to damage vulnerable populations, including but not limited to human rights campaigners, journalists, and dissidents. Use of cyber mercenaries is a challenge to accountability in cyberspace for determination of culpability for attack allows for deniability and diminishes adherence to agreed-upon duties. As a result, internet is becoming more dangerous. State actor-conducts an operation to purposefully disrupt, meddle with, impair, or damage computer systems or networks. State actors should be held accountable for their international and local legal duties.[6]

[3] Cyber Mercenaries: A new weapon in International Conflict, Michael Andruch 2021
[4] Human security centre, the rise of cyber mercenaries, Ataa Dabour, 15th May 2021
[5] Information privacy concern at individual, group, organization, and societal level - a literature review Dillip Kumar Rath and Ajit Kumar Department of Information Systems, Xavier Institute of Management, 2020
[6] Women's international league for peace and freedom February, 2021, Submission to the UN working group on the use of mercenaries regarding "cyber mercenaries" and their human impact

ISSN: 2582-6433

Types of cyber mercenaries[7]

1. APT Groups:

   Cyber security firm released a report in 2013 that established a relationship between the Advanced persistent threat group and government of China. Phenomenon of state sponsored cyber operations conducted by proxy. APT group is described as group that is involved in stealing of data, destruction in the infrastructure and carry out their project over months and years. Activities of these groups include espionage and commercial data theft, use intrusion techniques to enter the information system that includes foreign governments, agencies, ethnic groups, media outlets.

2. Cyber Militias:

   Civilian based network groups that voluntarily offer support to cyber operations and their objectives. But among these networks the activities, compensation, extent to which information is communicated varies.

3. Private software and technology companies:

   Few companies play a neutral role but other companies collude with authorities to provide data, information or manufacture spyware or any malware. An Italian company called the "HACKING TEAM" directly sold to the government the surveillance software that was utilised to spy on the people especially the activists, human rights defenders. The UAE based DarkMatter group manipulated the hardware of any surveillance units across the country to hack, locate any person.

4. Private contractors / Individuals:

   Can be classified as either on behalf of a beneficiary or on their own. These hackers have the responsibility of finding any sort of bugs or any kind of software vulnerabilities which help the manufacturer from protecting their software from intrusions. These individuals are referred to as "bug hunters." Few of them take advantage of vulnerabilities to either sell the information to competitors, criminals, or any other militaries. Statistics report show that the estimated money spent on illicit trade of such information is $25.1M from the private vendors.

[7] Trisha Ray and Antara Vats, "Cyber Mercenaries: A Call to Action for the Quad," ORF Occasional Paper No. 412, September 2023, Observer Research Foundation

ISSN: 2582-6433

5. Weapons Producers:

   The traditional producers of weapons resorted to digital era by resorting to offensive activities to benefit the clients. They support military operations, protect network resilience etc.

Non- State actors

The principal aim for state actors is collecting information and this is either left undetected the user for months, or years before carrying out or mobilising an attack. On this hand when state is on the affecting side, there are individuals, organisation on the other. The Internet is also a treasure mine of information which is utilised for social engineering and laying the framework for specific monitoring activities. Spyware entities, for example, at the first step of the surveillance chain, covertly profile targets by creating fake accounts on social media.[8]

The social media platforms, Facebook, YouTube are platforms that are useful for the civil population but are also capable of becoming spaces for repression and controlling of information. Facebook parent meta banned series of cyber mercenary and alerted around 50.000 people that were to be likely targeted by the firms accused of spying on activists, journalist worldwide. 1500 Facebook pages linked to the groups that were allegedly using public information online to using fake personas to build trust with targets or digital snooping via attackers. It had also contended about more than 100 countries have been targeted. The head of security policy Nathaniel Gleicher stated that accounts deleted were of Cobweb technologies, Black Cube, bell Trox, North Macedonian. These cyber mercenaries claim to target only the criminals and terrorists these activities of targeting are indiscriminate in nature and can include even journalists, activists, opposition members, regimes.[9]

"If terrorists can hire mercenaries, why not humanitarians?" The non-governmental organisations are increasingly turning/shifting towards the private sectors to protect and safeguard their property interest in all conflict zones, such as Save the children, Care. Military companies advertise services to NGO's, NGO trade association that are associated with the security forums of other countries that provide guidelines for hiring like InterAction and the European Security

[8] Trisha Ray and Antara Vats, "Cyber Mercenaries: A Call to Action for the Quad," ORF Occasional Paper No. 412, September 2023, Observer Research Foundation
[9] Facebook Data May Have Been Illicitly Used for Politics, and It Started with a Quiz, jerry Beilinson, March 17th 2018

ISSN: 2582-6433

Forum.[10]

In internet, there are even mercenaries known as hack back businesses. These computer firms target hackers or "hack back" against those who assault their clients' networks. The harm caused by a network compromise cannot be undone, but that is not the objective. They function as a deterrence. When hackers are selecting targets, they choose the softer target if they know one firm has a hack-back company behind it and the other does not. This is known as the active defence that has been declared illegal in many countries but other are questioning it as they provide protection for non-governmental entities. The WannaCry ransomware attack that took place in 2017, had targeted 230000 computers around 150 countries. The victims under these attacks included the United Kingdom's national health service, Telefonica of Spain, and Federal express of the USA. [11]

A classic example is the case of Vietnam were the individuals that were involved in the cyber operations, "force 47" was a cyber military battalion that consisted of around 10,000 forces. They were set up to fight against distorted and wrong information on internet. These groups harass people online by harassing people online through misinformation. Often, they work under private spaces or on behalf of any political actor, not necessarily a formal structure or agencies. [12]
Private military and security companies are another such incident. Tiger Swan in USA had targeted the Indigenous led movement of environmental activist that opposed the Dakota Access Pipeline through a military way to counter terrorism. It was hired by the owner of Dakota and had colluded with the state. It is claimed that they have used wide range of tools and instruments like phone tracing and social media surveillance to infiltrate the then ongoing movement to create some sort of disagreement between the activist, to collect data and to deter activism of future.

Issues arising out of cyber mercenarism

Entrepreneurial state-sponsorship of cyber mercenaries underscores the risks of non-apparent warfare. The issues arising due to identification and concerns related to anonymity afford for the mercenaries to engage in criminal or illegal activities by using of state funded natural resources.

[10] Mercenaries and War: Understanding Private Armies Today Sean McFate, National Defense University Press Washington, D.C. December 2019
[11] *ibid*
[12]Women's international league for peace and freedom February, 2021, Submission to the UN working group on the use of mercenaries regarding "cyber mercenaries" and their human impact

ISSN: 2582-6433

Hackers in cyber space are not bounded by any physical or geographical boundary that deepens the issue of locating the perpetrators of the activity[13].

Lack of a central regulation to govern cyber mercenaries has allowed for the growth of cyber mercenaries. The groups are unnoticed for a long term as they steal information required following which they abandon the network, usually called as the hit-and-run tactic. Lack of transnational legislation and organizing body to regulate or bring about any fundamental norms to promote peaceful further add to the struggle faced by the government to defend the exploitative use of the online aggressors.

Quad Nations and relevant legal regulations/agencies

Quad nations that focus on cyber concerns as they bear the cyberattacks are India, Australia, Japan, and United States(USA). These nations agreed to enter into Quad Cybersecurity Partnership. Lack of cyber security safeguards at both territorial and extra-territorial end caused disruption at economic level and other security concerns. The Quad leaders summit drafted principles relating to adequate processes and control methods in order to protect software, confidentiality, and integrity and to maintain and identify that software that require protection[14]. *In India,* the national cyber security policy of 2013 and Draft national cybersecurity strategy of 2021 led by the National Cybersecurity Coordinator which was an updated version of the security policy drafted of 2013. There use of term "cyber mercenary" is undefined but the threat is under surveillance due to the increase in the hack for hire groups. The Indian government has signed several MoUs that majorly focuses on the cyber security concerns. Collaboration with regional groups like that for Multi Sectoral and Economic Corporation and the South Asian Association for regional cooperation that depicts the shifted focus on cyber security matter to address the challenges in the cyber domain, thus shows an evolving landscape.

Other bodies in India for implementing these strategies and regulations is the National cybersecurity coordinator, National information protection centre, National technical research organisation.

[13] Mercenary-Related Activities in Cyberspace CyberPeace Institute October 20, 2021
[14] Trisha Ray and Antara Vats, "Cyber Mercenaries: A Call to Action for the Quad," ORF Occasional Paper No. 412, September 2023, Observer Research Foundation

ISSN: 2582-6433

Major cyber mercenary attacks

1. In 2020, the blackberry research had unleashed a new APT group not linked to any government but have activities similar to the traditional APT's. Mercenary groups of such APT style are increasing and by suing mercenary as their proxy the real user or hacker can protect the identity[15].

2. The cyberattack on Bangladesh Bank serves as an example of both the variety of hackers and the difficulties that outside parties might provide. Hackers from the Lazarus Group attempted to steal $951 million from the Federal Reserve Bank of New York account of the Bangladesh Central Bank in 2016. They did this by connecting an IP address in North Korea to a server in Europe, which they used to run systems they had previously compromised. Security hackers gradually got to know the day-to-day operations of the bank before they fraudulently instructed 35 high-value transactions across the SWIFT network. Hundreds of financial organisations use the SWIFT network, a worldwide information system, to exchange money. The total was $101 million, even though the hackers were only able to fulfil five of their requests. However, a $20 million transaction was stopped because one of the transactions had a typographical mistake. It was purportedly determined that the hackers who launched the attack from Bangladesh were associated with North Korea.[16]

3. The Chinese APT group that was named by researchers as the quad response echo had hacked into the electricity supply control systems and along with it installed malware that intermittently turned off Mumbai's electricity supply including the hospital electricity generators that were used for emergency to keep the ventilators working for the COVID affected patients.[17]

4. The official website of Ministry of health and family welfare was breached. Resulting in retaliating the decision that were taken by the Indian authorities "to comply with price ceiling that was approved by the G7 countries for Russian oi and to not violate any sanctions" was by a pro- Russian hacker group, the Phoenix in 2023. [18]

[15] *ibid*
[16] da Cruz, José de Arimathea and Pedron, Stephanie () "Cyber Mercenaries: A New Threat to National Security," International Social Science Review: Vol. 96 : Issue. 2 , Article 3.
[17] *ibid*
[18] *ibid*

ISSN: 2582-6433

5. The Unique identification authority index was targeted by Chinese state sponsored group. The index is the countries national biometric Id aadhar card that was attacked and also had targeted the Times group which followed after the border clash in 2020[19].

6. The Google security team in 2009, found traces of cyber-attacks in their internal system. An employee as claimed to have had searched for Chinese names on the internal discovery portal. Security experts traced down the hackers/attackers by employing an MSN chat message with google link to photo-sharing site. The attackers moved into the core network of Google, identifying their interest in human right activists like that of the Tibetans. The attackers exfiltrated the source code and had undertaken search for the attackers. Investigation and evidence gathered were sufficient to prove that the Chines government or agents were the mastermind behind the attacks. This captures the uncertainty in distribution of responsibilities against state adversaries. Google combined business decision by publicly bringing it on the Chinese government knowing off the economic and political implications.

Conclusion

The biggest obstacle in addressing the issues arising and the challenges by cyber mercenaries is the absolute requirement of research in the field and exposing the attackers and finding suitable and efficient measures to prevent targeted cyberattacks conducted by the state sponsored malware spyware by the private companies or the non-state actors. Mercenaries enable strategies of deception; clients hire them as agents. Their covert actions with their zero footprints have maximized their plausibility of denial.

While the investigation is still underway, preliminary findings indicate that the development of cyber mercenaries in India poses a significant threat to national and international security. It emphasizes the need of QUAD nations working together on cybersecurity and the need for improved individual data protection measures. A scheme or design as to the type of actors that must be classified as cyber mercenaries and their scale of responsibility that will also determine liability has to designed by the Quad Senior Cyber group.

[19] Mercenaries and War: Understanding Private Armies Today Sean McFate, National Defense University Press Washington, D.C. December 2019

ISSN: 2582-6433

It is too late to ignore, regulate or ban the private military industry. Mercenaries is a dangerous trend but is invisible to an individual using internet on an everyday basis. They offer means of war online and anyone can transform that into future warfare. The mercenaries are here to stay.