Journal of Legal Studies and Criminal Justice
e-ISSN: 2708-9606; p-ISSN: 2708-9592

Legal Studies & Criminal Justice

Unravelling the translucent theories on Espionage: A periodical study on Crime and Security

Abhisekh Rodricks[1], **Jyoti Puri**[2]
[1,2]Amity University Kolkata, India
Correspondence: abhisekhrodricks@gmail.com

Abstract

The concept of human based Espionage has grown between nation-states since the time of ancient civilisations thus the same is not a new phenomenon, but in the last few decades the globe has moved into an absolutely new dimension of spying through artificial intelligence and internet system aptly known as cyber espionage. This futuristic form of espionage has brought the global sphere into their control tackling national security, affecting the economic and political relationships between nation-states as well as changing the shape of modern warfare. Therefore, in spite of the advantages brought about by modern technology, there is a whole new set of problems as well. This paper provides some background on cyber espionage, including what it is, how it works, how it is used, and who is using it. This paper tends to analyse and identify how cyber espionage is affecting the world today and describe some possible methods for nation-states to create policies keeping in mind citizen privacy against cyber-attacks.

Keywords: cyber espionage, nations, policies, security

Introduction

The concept regarding Espionage and Counterespionage and its multifaceted practices has been in practice since time in memorial among various kingdoms and civilisations in history. Espionage and spying are one of the very ancient professions. It is at least as old as the scriptures of The Holy Bible, wherein the chapters of Joshua refer to the spies which were sent by Joshua into Canaan before he led the Jews across the River Jordan. Espionage and counter espionage are very often loaded with misnomers and deceptions commonly portrayed in the concept of glucan novels and films, every stage of a broader game of espionage and counter-espionage that are integrated into a process which can be derivate as the intelligence cycle. Furthermore, lying and deception occur even within the ranks of the properly identified and the absolutely so-called patriotic members of the departments of intelligence, security and also policymakers, on tasks as seemingly benign as joint collaborative practices, routine intelligence reports. The concept of Espionage requires that the identification patterns will explore each of the five stages of the intelligence and informational patterns, where lying and deception creep in and then move into compel certain activities. In observing such practices, counter-espionage would then have to be addressed not as a separate intelligence-related activity, but at the onset and throughout: as it is was within the intelligence cycle.

The concept of espionage under: - international law

The domain of International espionage consists of a very vital concept in terms of diplomatic relations i.e. access, on behalf of a state with regards to the information that is most often held by the archives of another state and is more commonly considered to be as confidential or strategic, to the armed forces, internal security, diplomatic relations or economic field. This clear conception has evolved to include within its ambit, surveillance programs implemented by intelligence agencies for the benefit of individuals as well as for the purpose of trade related company-to-company industrial espionage.

During a long span of time the system based on espionage essentially took place within the physical space, during the present century, it primarily occurs within the sphere of the coveted region named cyberspace. It should also be noted that, against common assumptions, the notion exclusively refers to the gathering of information and does not refer to covert dissemination pattern carried out by the security forces more generally. Although such operations are a very antiquated and common practice, this concept has been paradoxically unregulated by an absolutely unique and coherent legal regime under international diplomatic regulation. Only the status and identity of these

agents in times of humanitarian crises is, in fact, subject to basic and profound of international regulation. More so, in recent times, the legal issues put forward by espionage have largely been ignored by the doctrinal literature. It was only in the event surrounding the Cold War—in light of various milestones which led to the oppression of the United States and the USSR—these events brought the real interest in interstate spying activities on territory-based landmass and sea, and in air and space. The analyses which was drawn by scholars actually focused on general principle of international law and on the tenet of state as laid down in the Montevideo convention that is the concept of sovereignty of state[i] which is basic for the recognition of a state within the domain. International scholars, most of whom who, being former diplomats who played an important role or most precisely. This is very often resulted to doctrinal analyse that disseminated the plurality the legality of intelligence-bureau across the world. That being said, more substantial literature also exists. In latest research, the particulars, have started to questioning the compatibility of surveillance practices with human rights law. In the case of united states of America, the 9/11 attacks, the problem of espionage has, gained new moments due to the implementation of new parts of surveillance programs for the purpose of fighting terrorism. The betterment of new technical issues and communication media has, likewise, heightened possibilities for mass surveillance. In legal area, discussions have mainly focused on the legality of espionage under international human rights law. Forms of espionage have become more diverse and sophisticated, involving acute array of participants and stakeholders. Due to this evergreen diversity, and of the absence of a single, unspecified legal regime under international law, the problems amplified by the system of espionage require the reinvestigation of a different set of rules: sovereign theories ; non-intervention; forced based approach; sea, air, and space law; human rights; international economic law; global law on crimes; etc. Basically, two categories of approaches can be identified in the doctrine. The first is related to an international approach, which investigates espionage in a transversal approach and in its multifaceted dimensions. The second, one was based upon the concept of sectorial approach that tends to analyse specific espionage activities in light of a particular set of regulations.

Cyber espionage or cyber spying

The recent trends of Cyber espionage or cyber spying is the act of obtaining an individual personal, sensitive, or operatorial proprietary information from individuals without their consent or idea. In an ever-growing transparent and technological civilisation like ours, the ability to control the private and declassified information an

individual knowingly and unknowingly reveals on the social networking and the ease of external ability of others to access that information are a growing concern. This brings external storage and third-party email, social media, search engines, data mining, GPS sensing, the explosion of android usage, and many other technology considerations. In the age of big data, there is an enlarging concern for private issues surrounding the storage and misuse of individual data and non-consensual mining of private information by corporate sectors, criminals, and governments. Concerning the growing threat of cyber espionage in the global technological world, Sigholm and Bang write that unlike ritual crimes, companies cannot call the police and expect them to continue cyber criminals. Affected platforms play a major role in each and every investigation because it is their process and data that are being stolen or leveraged. The issues against cybercrime must be waged on a major basis, regardless of whether the criminal is a rogue hacker or a nation-state.

In 1968, the US government passed the Omni-bus transport Crime Control and Safe Streets Act, which is a kind of a telegraph-based law is commonly known as the Wiretap Act. This law is basically illegal for any person to will fully use an electronic or mechanical device to intercept a verbal communication unless an important consent was given or if the interception occurred during the specific course of business. In 1986, Congress passed the Electronic Communications Privacy Act[i] (ECPA) which amended the original Wiretap Acts and also introduced the Stored Communications Act (SCA) which basically prevents outsiders from hacking into facilities that are used to store in digital communications. These parts of legislation form the cornerstone for elaborating protections against cyber espionage in the age of big data and social networking. In the concept of US privacy laws, the European Union (EU) has adopted an accurate legislation governing the collection and processing of personal information. This ensures that individual data is the main process within acceptable privacy limits. Compared to the EU, and the USA has relatively few laws that enforce private information. The USA has mostly relied on industrial rules regulations and practices to ensure privacy of personal data, and the most evident feature of EU rules in relation to the USA has been the prohibition of the transfer of individual data to countries outside the EU that don't assured an adequate level of protection EU law confirms that the collections, storage, or ample of information relating to individual's life interferes with the right to private life and therefore that requires summarization. Ironically, as we become a more technological dependent society with increased public surveillance, data mining, transparency of private information, and social media, we come to expect less privacy and are consequently entitled to less of it. This leads to the difficult question of how

much privacy we as individuals can "reasonably" expect. Recently, the Jones v. United States case[i] challenged the existing privacy expectations over police surveillance using a GPS that monitored the suspect's location. As the normalcy ideals of warrantless surveillance which expands and our expectations fall, thus absolutely allowing this type of surveillance to become more "common." This results in a move toward limitless police powers. These declining expectations are at the heart of the Obama administration's argument in this case, where it affirms that the government is free to track citizens without warrants because citizens "expect to be monitored"

Requirements

As a policy-driven enterprise, this is the important phase of the knowledgeable cycle. Originates with the policy introducer who set the overarching international and national intelligence gathering scheme. They are identifying the motives and double dealing of other actors (e.g., Does any country have enzymatic weapons?? They claim they do don't have? What kind of banks are laundering money for terrorist Cal financiers? It also involves the needs to guard individual's idea and deceptions. Guards against spiteful agencies, individual's intelligence collection activities (vs. satellite intelligence collections, etc.), are called counter-espionage. However, the counter-espionage is a setting of a much larger effort to guard one's idea, motives and deceptions are formally known as counter-intelligence (CI).

The needs for counter-intelligence is conducted for actions to guard against threats the from outside country's intelligence community (few agents from spiteful organizations) and from inside it(spy). The CI operation is to protect state national and international secrets, including their sources and resources and the means by which they were gathered. In this process, CI agents must overcome the habit to trust others, including those people who are the part of their own organizations and also who have passed their security clearance screenings to assume that virtually anyone could be an agent.

There are two sets of security, present in united states of intelligence organisation, to protect CI. The first way is for people's detail screening. This involves background checks of the applicants and also current agent, to weed out those whose adherences are deemed too dangerous to be entrusted with the national secrets. These types of checking involve verbal questioning with the use of a polygraph device. The polygraph device measures physiological changes—can be changed/defeated by the persons those who are giving interview. For instance, Aldrich Ames, among the most famous of all CI spies, passed ample of polygraph interviews during his period, during

which he fed high amounts of intelligence to his Soviet holders.

The second CI security is the basic system where important information is labialized (e.g., confidential, secret report, top secret of agencies) and securely saved according to few reports related to Lying and Deception they basically posed were they have to compromise. Even within a given division tier, materialistic stuffs are further compartmentalized. Where the access to information is generally permitted on a need to know basic reports. The future goal of this procedure is traducing to a single individual, access to secret information, hence reducing the damage that could be caused by any given source of secret information leakage. Critics of this basic procedure that points out the normal used deception, for concealing from the public illegal activities and some ethically professional mistakes made by governmental authority.

Covert Action

Covert actions are basically those policies, which our nations take forward to sketch agendas in different ways that is because they cannot deny the responsibility. These actions were aimed by nation's adversaries, involves many activities like paramilitary missions, planting wrong news reports, and spreading meaningless rumours. If the deception was invented by our nation's adversary, it can give a huge result in que veut dire military or diplomatic consequence. At the minimum stage, the intelligence borrows a compromised covert action in a limited insofar as the corrival is made aware of the breaks in their structure and they might take steps to shore up their personal counter-intelligence around such vulnerabilities.

Collection

The main phase of the intelligence cycle, and collection are commonly associated with espionage. In this important phase, government "agents" are called case officers—assume one of two kinds of deceptive cover reports to explain their presence in other nation. However, a case officer deals that type of cover is likely to be doubted of connection to their government's surveillance services. Therefore, some case officer are needed for "non-official cover" (NOC, pronounced, "knock"), whereby they masquerade in a mysterious occupations (though humanitarian law restricts cover as clergy or members of the Peace Corps)[i].One of the main NOCs is that of a journalist: a person who, by trade, has reasons for foreign travel and to meet with a wide range of people.

When cover, case officers starts recruiting and handling a network of spies—formally known as agents—during which they stay sensitive to the possibility that their own spies are deceiving them. An officer could be a "sway" bait held out by a antagonistic

intelligence service hoping to the process for themselves a double-agent. Partially, agents might fabricate exaggerate the important reports they confront to case officers, in hopes of dealing with the profit (monetarily and emotionally etc) along with their associations and with them. Consequently, case officers verbally ask agent's motives, how agents have power to access information, and the validity of that information. Basically, the case officers must have a balance risk to intelligence security with the risk of lost intelligence reports.

Theoretical Information from the important phase is not accepted intelligence until it has been groomed for use—which often includes translating, coding, decoding, or rechecking it in context with other secretive information—as the major part of the phase of the intelligence cycle. In extending intelligence assessments, the U.S. uses a juridical analysing system, whereby different web reports are Lying to intelligence agencies, or different working teams within an agency, derive self-dependent projects to be reconciled. by the jurist, if not their egos, depend to few degrees both upon "being right and being noticed by their mentors for being right. Consequently, competing analytical teams occasionally will get one another by adding false or weak analytical list (so-called "false hostages")[i] in their first stage, draft essential reports: those are seized and acknowledged by opposing team in exchange for inclusion of their pet points in the final intelligence curriculum.

From few reports we have to gain attentions, analysts occasionally deceive to the makers of policy by breaking the truth or elaborating the importance of their assessments. In the extreme, analysts round their assessments to describes the policymakers that what they think or what they want to listen (known as "politicization"). Additionally, the policymakers randomly take information about the context from sound intelligence reports to deceive in the public in ways that suit their own individual agendas (known as cherry-picking).

In another phase of the intelligence cycle, intelligence information reports are circulated to consumers within the help of government. These are the normal range of reports those are tailored for a particular user (e.g., the President's Daily Brief) to extended for broader governmental readership (e.g., the Senior Executive Intelligence Brief), to those who approved for release to the citizen (few national intelligence estimates). As a counter-intelligence measure, each type of information reports is given in classification level and also that is saved accordingly.

In the last phase of the intelligence cycle, ideally the policymakers give feedback to the intelligence community, regarding the extent to their intelligence needs or reports where they met, that includes requests for addition intelligence. However, this is not a

proper system: one that opens the door for both the intelligence community and to those who make policy to succumb to self-deception. Policymakers define themselves when they mistakenly assume that the intelligence community understands their intelligence request and needs. the intelligence community describes that when it concludes to lack of feedback from policymakers is indicative of policymaker comprehension, contract, or satisfactory service by the intelligence agents they have to receive.

Vulnerable Technologies

Gadgets have become a common fixture of daily life, and the enormous amount of personal data stored on these devices has led to unforeseen difficulties with the interpretation of laws meant to protect privacy. Current legislation has actually focused on defining a smart phone as an extension to an individual's home for the sake of protecting sensitive and secretive information. In 2009, the Supreme Court of Ohio issued the most clear-cut case which held that the search of a smart phone incident to an arrest is unreasonable under the Fourth Amendment. The court held in State v. Smith[i] that because a smart phone allows for high-speed Internet access and is capable of storing "tremendous amounts of private data," it is unlike other containers for the purposes of Fourth Amendment analysis. Because of this large amount of personal information, its user has a "high expectation" of privacy. In short, the state may confiscate the phone in order to collect and preserve evidence but must then obtain a warrant before intruding into the phone's contents.

Smart phones have evolved into intimate collections of our most personal data and no longer just lists of phone numbers, the type of data that has traditionally been kept in the privacy of our homes and not in our pockets. The phenomenon of social media has raised a host of security and privacy issues that never existed before. The vast amount of personal information displayed and stored on sites such as Facebook, Snapchat, My Space, and Google make it possible to piece together a composite picture of users in a way never before possible. Social networking sites contain various levels of privacy offered to users. Sites such as Facebook encourage users to provide real names and other personal information in order to develop a profile that is then available to the public. Many online dating sites allow people to remain anonymous and in more control of their personal data. This voluntarily divulgence of so much personal information plays into the debate over what kind of privacy we can "reasonably expect. "In 2003, an individual named Kathleen Romano fell off an allegedly defective desk chair while at work. Romano claimed she sustained serious permanent injuries involving multiple

surgeries and used Steelcase Inc[i]., the manufacturer of the chair. Steelcase refuted the suit saying Romano's claims of being confined to her house and bed were unsubstantiated based on public postings on her Facebook and Myspace profiles which showed her engaged in travel and other rigorous physical activities. When Steelcase attempted to procure these pictures as evidence, Romano opposed the motion claiming she "possessed a reasonable expectation of privacy in her home computer" Facebook also opposed releasing Romano's profile information without her consent because it violated the federal Stored Communications Act[i].

Conclusion

The concept of Espionage and counter espionage though being ancient both in terms and practice, still is a secretive practice which is well coveted in most parts of the world, away from public outlook and political interference, basically stating essential reasons for its impugned importance. The reason being that it might threat national security and state sovereignty. But when there lies a conflict of vigilance and personal data in the present era of technology one has to balance between the two in terms of privacy laws , individual liberties and national security pertaining to a state especially where selective espionage is concerned .Thus it is invaluable to prioritize the scheme and scope of the categories of espionage and also its varied classification, use in the world among states, agencies etc for the creation of a better ,secured and sustainable world.

References

[i] Montevideo Convention on the Rights and Duties of States. -1933

[i] Electronic Communications Privacy Act -1986

[i] Jones v. United States: 362 U.S. 257 (1960)

[i] https://www.hrw.org/legacy/wr2k6/wr2006.pdf

[i] https://www.alaskaanthropology.org/wp-content/uploads/2016/04/AJA-v111-2.pdf

[i] State v. Smith - 210 Conn. 132, 554 A.2d 713 (1989)

[i]https://www.jacksonlewis.com/resources-publication/individuals-private-social-networking-sites-are-not-exactly-private-new-york-court-rules

[i] Electronic Communications Privacy Act of 1986.