Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 5, 2026

FROM HACKING DEVICES TO HACKING MINDS: PEGASUS AND THE RISE OF CYBER-PSYCHOLOGICAL WARFARE

Dr. Zeeshan Zaighum[*1], Dr. Muhammad Jawed Aslam[2]

[*1]*Assistant Professor, School of Media and Mass Communication, Beaconhouse National University, Lahore, Pakistan*
[2]*Associate Professor, School of Media and Communication Studies, University of Management and Technology (UMT), Pakistan*

[*1]zeeshan.zaighum@bnu.edu.pk, [2]jawed.aslam@umt.edu.pk

DOI: https://doi.org/10.5281/zenodo.20178798

Keywords
Fifth Generation Warfare, Information Operations, Surveillance, Pegasus

Article History
Received: 19 March 2026
Accepted: 29 April 2026
Published: 14 May 2026

Corresponding Author: *
Dr. Zeeshan Zaighum

Abstract
The introduction of fifth-generation hybrid warfare has changed the character of information warfare (IW) to a multi-faceted battle space. In this warfare, cyberspace capabilities and psychological operations work together as an integrated whole. This paper analyzes the convergence of IT and IP operations through the example of Pegasus Spyware. In today's cyber operations are no longer limited to just technical domain and/or espionage but also include cognitive manipulation, behavioral targeting, and social engineering techniques. Through a qualitative case study approach; this research investigates the forensic reports, investigations undertaken regarding Pegasus operations, intelligence assessments, and leaked spear-phishing messages, with an emphasis on thematic analysis to identify patterns of political persuasion, emotional exploitation, cognitive targeting, and use of social engineering found in attacks using Pegasus. It also shows that Pegasus was not simply a cyber-espionage weapon but rather part of a complete cyber-psychological weapon system that is used to manipulate how targets behave in order to achieve greater operational success. The research further concludes that this combination of cyber and psychological operations acts as a force multiplier within the framework of contemporary information warfare.

Introduction
William Lind argued that in future, media and information would be a key factor in warfare in both operational and strategic levels. Psychological Operations (PSYOPS) would be planned in a manner where the main target would be the people of an enemy state. The major objective would be to turn people against their own government or the state itself during the new form of war (Zaighum & Rasool, 2023). Television would be a more powerful weapon than any other military weapon of hard power (Korypko, 2015). The emergence and widespread penetration of internet has primarily made the access to the information high equally accessible for all countries. Unlike traditional hard power disparity where few countries were far more technologically advanced than the rest of the world, the internet has globalized the information highway. However, along with its emergence, it has also changed the way countries exist and co-exist. The informational revolution has left its influence in all spheres of human experience. Warfare is no different. The idea of 'Hybrid War' is also a conceptualization of the effects the information revolution has brought in the warfare. Hybrid Warfare can be defined as a war where several types of warfare tactics are used at the same time. Owing to the adaptive nature of the warfare, Hybrid Warfare can be

multifaceted and multi-dimensional use of traditional and modern warfare techniques. In modern times, the traditional characterization of scales of war (small, medium, large) and nature of war (regular or irregular) cannot be applied to Hybrid Wars. Newer generation (fifth) war would encompass all the traditional and modern actors of warfare and would comprise the operation area of the warfare. These include state and non-state actors, terrorist groups, militaries and militia. The most significant aspect of this generation is the use of information and communication technology where the most colossal damage to an adversary would be caused not by non-state actors but from state actors. This could be used against even the most powerful countries of the world (Johnson, 2017).

Problem Statement

Traditional Information Operations lack integration, making them reactive, while adversaries synchronize cyber, psychological, and influence efforts for greater impact. (Vertuli & Loudon, 2018)

Integrating cyber capabilities with psychological operations is essential for modern warfare, enabling precise psychological targeting and influence at scale cyberspace serves as the primary battleground where psychological and technical capabilities must be unified to conduct effective, targeted influence operations (Military Review, 2024).

The Pegasus revelations exposed the necessity of integrating Information-Technical (cyber warfare) and Information-Psychological (cognitive manipulation) operations, leading to a doctrinal shift in military strategies. Modern defense policies now synchronize cyber capabilities with psychological tactics, enhancing influence operations and operational effectiveness (Vertuli & Loudon, 2018).

Research Questions

1. How do modern military and intelligence frameworks integrate Information-Technical (cyber warfare) and Information-Psychological (cognitive influence) operations?
2. In what ways does the Pegasus spyware case demonstrate the convergence of cyber and psychological operations in contemporary information warfare?
3. How does the integration of cyber and psychological operations act as a force multiplier in cyber espionage and influence operations?

Literature Review

Information Operations are designed to stimulate actions, mindsets and behavioral patterns of a population. This is done by affecting their otherwise rational thinking, conscious engagement and manipulating their decision-making mechanisms. According to a report published by the US Army War College, information operations are designed to influence the behavior. Furthermore, these operations are carried out as per the dynamics of an information environment and are associated with the concept of national power (US DoD, 2011). Information Operations are cohesive engagement during army operations through Information Related Capabilities (IRCs). The IOs are employed along with other activities to distress the decision-making process of enemies or potential through influence, disruption, usurpation or corruption techniques. Information Operations are also the integration of the deployment of hard power and inclusion of information activities aiming at the perception and will power of enemies. Just like a fire support mechanism in an operation environment, Information Operations help generate desired results through integration of various capabilities in an Information Environment (DoD, 2013).

An official document of US DoD (DoD, 2014) presents a scenario of visualizing an information operation. The scenario poses a country where an incumbent government is being overthrown by enemy. The government is deemed unfit to run the state and safeguard its citizens. The enemy is using both deadly and non-deadly means to achieve its goals. The main objective of the force is to protect the government from being ousted. The assets to achieve the goals are several. Diplomacy is the first mean- writing a demarche, reaching out to international and regional citizens to confront movement's legitimacy, engaging with public and lobbying. The second asset is information- media can be

an effective tool to shape and mold public opinion. News generating activities and news itself help achieve program goals. People rely on media for different sort of information and therefore, media has the power to build public's information repertoire. Strategic communication (Stratcomm) is also another mean of information assets. Agenda setting, propaganda, advocacy, rhetoric can also be effective tools. Economic and financial assets are also influential in such operations- use of trading organizations, corporate sector, multinational organizations are also helpful. The economic measures can be two faceted: supporting the incumbent government through financial support, trading agreements, and announcing investments, and sanctioning the adversary. This puts an adversary in the back foot. The role of diplomatic Track-II organizations can be also effective. The last mean is the military- planning a task force operation, tactical attack, military deception etc. The use of broadcast and digital media, utilizing/attacking government cyber infrastructure, engaging with leadership are other ways to achieve the goals (DoD, 2014).

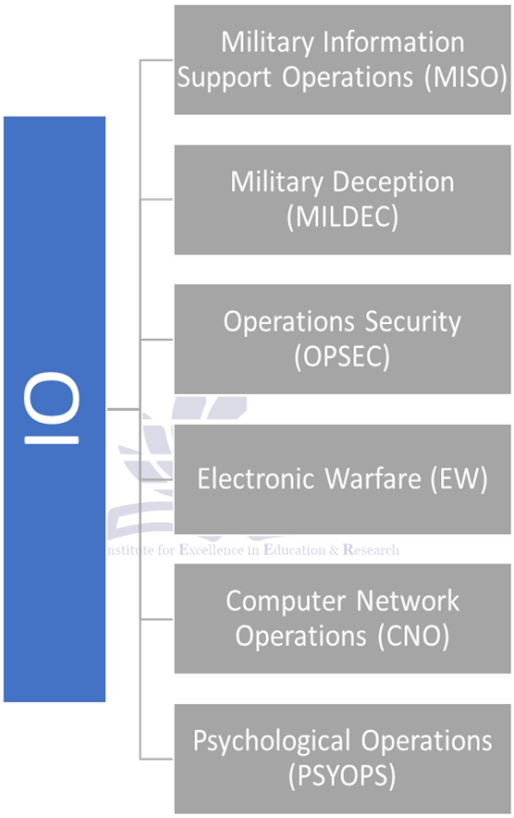


Figure 1: Traditional Capabilities of Information Operation (DoD, Information Operations , 2014)

Military Information Support Operations (MISO)

These operations are designed to establish desired favorable opinions and perceptions regarding military in the global information environment. The information activities in such operations are designed to be cultural and normatively appropriated for target audience. The purpose of such MISOs includes to triangulate a positive relationship in military operations, public diplomacy and public affairs.

Military Deception (MILDEC)

Military Deception is hard core a strategic communication action aiming at deliberately misleading adversary or an unfriendly organization to take ill-informed actions. MILDEC disrupts adversary's decision-making process and take poor actions in order to support own goals. MILDEC creates a pseudo environment through a twisted projection of reality. MILDEC is both a mean and a process. As a process, it includes a planned and systemic approach aimed at targeting individuals in physical, informational, and cognitive domains.

The major objective remains tactical manipulation of adversary's decision-making process. MILDEC also plays an important role during a military operation by covering vulnerabilities, counter deception, diversion, and engagement.

Operations Security (OPSEC)

Operations Security (OPSEC) is another traditional capability of Information Operations. OPSEC includes protection and security of critical information. OPSEC aims at engaging any information that can jeopardize an ongoing or a planned operation. The scope of OPSEC is to secure operations security through information, and misinformation, ensure tactical security, maintain the advantage of surprise etc. OPSEC is planned in order to diminish operational certainty, eradicating indicators of mission, destroying adversary's information collection network, disrupting enemy's operational indicators' perimeters through attention diversion and planned camouflage, false operations, and in the end distorting an adversary's counter analysis mechanism through planned leaks.

Electronic Warfare (EW)

Electronic Warfare is a hardcore hard power capability. These actions are not related to cognitive or information domains but remain strictly limited to physical domain. EW operations include military operations in electronic magnetic spectrum. Jamming and paralyzing an adversary's radars, communication signals, capturing electronic signals are included in this warfare.

Computer Network Attacks (CNO)

Computer Network Attacks (CNO) are also called Cyber Attacks/Operations. These operations include attacking and protecting critical cyber and computer infrastructure. The offensive operations are conducted through hacking, espionage, infiltration and disruption of an adversary's critical cyber infrastructure, database, website or even official handles on social media.

Psychological Operations (PSYOPs)

Psychological Operations (PSYOPs) are one of the oldest forms of information warfare. The cognitive dimension of IOs is based on psychological warfare. The operations in PSYOPS include building narratives, propaganda campaigns, misinformation, disinformation, malinformation, lies, truths, half-truths, twisted facts, coercion, intimidation, greed etc.

Information is a full spectrum of warfare. It is a domain warfare because war is also fought in this sphere. It is a function of warfare because war, its planning and execution rely heavily on collection and dissemination of information. It is a domain of warfare because war can be won or lost on the bases of information. As a weapon, information can colossally destroy the will of an adversary to fight. In both Kinetic Warfare and Non-Kinetic Warfare, information has always had key importance. In an operation environment, where forces both friendly and adversary fight against each other they are always face each other in information sphere as well. In modern warfare the omnipresence of information and communication technologies have genetically transformed the concept of information warfare. The amount of information that is created today is unprecedented in the history of information warfare. The democratization of technology has meant that there is an equal and easy access to the basic platforms of information collection, production, and dissemination. More importantly, there is low disparity with regards to the access of such platforms. Therefore, state and non-state actors, friendly and unfriendly forces, use information communication technologies for own interests. From recruitment and radicalization of vulnerable groups to the dissemination of fake news, information and communication technologies have emerged as battle ground of information operations. Such operations have seen immense success because of the lack of digital media literacy and audience's dependency on such platforms for information. Social and digital media platforms have created a reality of their own. As Thomas Theorem suggests, if men define situation real, it is real in consequences (Thomas & Thomas, 1928). The theorem can be

supported by the evidence found during the Brexit Elections. A report highlighted that in 2016's British referendum concerning Brexit, Russian supported accounts published hundreds and thousands of tweets on the election day. These tweets played the role of catalyst and encouraged individuals to vote in favor of the withdrawal. A total 3800 accounts were found to be linked with Russia which published similar tweets (Grčar, Cherepnalkoski, Mozetič, & Novak, 2017).

Information Operations have following three dimensions. "Connectivity" is the first dimension and means the connections of tangible communication devices. It also includes intangible affinity of people through relations, social groups and networks. The second dimension is 'content' and can be categorized in two opposite directions: inputs and outputs. Inputs include desired behaviors, stimuli and outputs include reactions, emotions, decisions, actions, behaviors. In both directions, content is any piece of information that is created to exchange meaning. This includes images, texts, databases, activities, actions, behavioral patterns, silence, inactions, visuals, graphs, news etc. The third dimension is 'cognition'. This dimension is intangible in nature. This dimension is human brain. All the knowledge, information, emotions, opinion known to a person are processed, interpreted, and stored in the cognitive dimension. Unlike other dimensions, human cognition cannot be attacked directly. Attacks targeting human cognition are planned in the informational and physical domain and therefore, cognitive dimension is attacked indirectly. Human cognition is comprised of different units of information, perceptions, opinions, beliefs, norms etc. These units operate like a window that can be a mean or even an obstacle while having a perspective (US DoD, 2011).

The three dimensions of Information Operations help operational objectives of the three dimensions of information environment through the following traditional capabilities of information operations (ATP, 2018). Moreover, psychological operations can support other traditional information operation capabilities. The following figure explains that any information operation is a part of a psychological operation or may produce psychological effects.

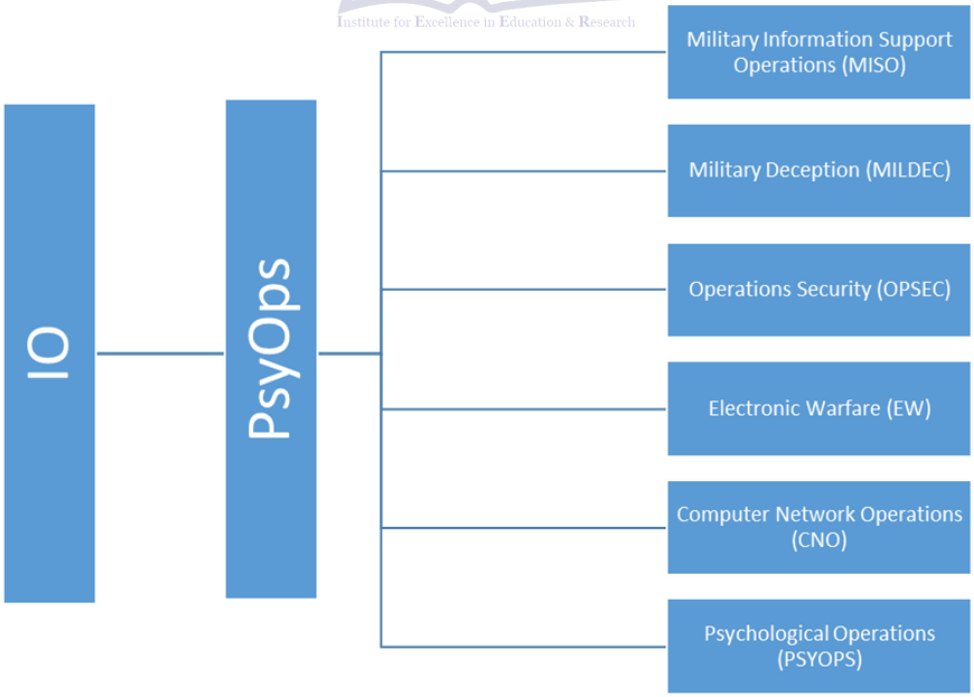


Figure 2: All IOs are supported by PsyOps- developed by the researcher

Approaches of Information Operations

Traditionally, there are several Information Operations techniques and approaches adopted by different militaries in the world. Few of them are as follows.

Maskirovka

It's an old Russian military technique. A synonym to deception, Maskirovka supports an ongoing or a planned military action. The main focus of Maskirvoka is to keep the element of surprise alive. Furthermore, through exaggeration of military deployment number, it tends to disrupt an adversary's will to fight. It also exacerbates false operation environment through the use of dummy weapons, deployment of prototypes in the operation environment, and thereby, psychologically influencing an adversary through intimidation. Caddell (2004) explains the following techniques of Maskirovka.

Maskirovka 2.0

Maskirovka has been a Russian military doctrine from the start of the twentieth century. It has remained a military philosophy during the cold war era. It has also brought innumerable desired results to the Russian military. Nevertheless, in this era of digital technologies, Maskirovka is far from over. Russian military and leadership have used maskirovka in Georgia, Ukraine, Syria. In Maskirovka 2.0, new techniques have been incorporated with old practices. The new techniques include intimidating governments and militaries, propaganda, media exploitation, intimidation through natural resources, weaponizing political activism, provocation, cyber warfare, diplomatic attacks in the whole MPCEI (Military, Political, Civil, Economic, Informational) spectrum. Maskirovka 2.0 paved the way for Russian military action in Georgia in 2008. In Syria, Russian support to Assad's regime to counter terrorism also reflected the concept of Maskirovka 2.0. Assad's call for an intervention legitimized Russian actions and therefore, Russia tried to establish the image of a peace keeper (Roberts, 2015).

Reflexive Control

Reflexive control is another doctrine and approach of designing and executing information operations in information warfare. The main focus of Reflexive control is to encourage and provoke an adversary to take an action that is already predetermined by the actor. This is done by leaking a desired piece of information, spread of false news and propaganda. Reflexive control relies heavily on behavior and elements influencing behavior. Therefore, Reflexive Control is about directing and willfully managing adversary's reactions. Reflexive Control also encompasses perception management. Attributed to Vladimir Lefebvre, Reflexive Control is a process where an actor deliberately transfers certain stimuli towards an adversary to take an action or makes him respond accordingly (Giles, Sherr, House, & Seaboyer, 2018). Distraction: create a real or imaginary threat to the enemy's flank or rear during the preparatory stages of combat operations,

Reflexive Control is attributed to the Russian military doctrine Maskirovka. Nevertheless, the US has also been argued to use reflexive control as a strategy. Strategic Defense Initiative (SDI) was introduced in 1984. The main purpose of the program was to conduct research on modern aerospace technology to counter Russian threats. The then President Reagan announced new national security policy. SDI has also been attributed as 'Star Wars' project. According to (Thomas T. L., 2004), the announcement forced Russians to react in a way that was already predetermined by the US and thereby, the US was able to control Russian reflexes.

With the growth of traditional media followed by the emergence of internet and digital media platforms, information operations have transformed into multifaceted activities. Wars are now fought on the battle field and also on the information domain. Interestingly, Keenan (2001) argues that the new information and communication technologies would not only change the way militaries fought or political powers steered political affairs, but it would also provide a sphere for international citizenry where any one from non-governmental organizations to civil activists, from militaries to militia would have free access to unprecedented opportunities.

The use of internet during the Kosovo War of 1999 paved the way for the contemporary

weaponization trend of internet in warfare. Both state and non-state actors used internet. Propaganda aimed at vilifying the other was spread over the internet. False information and fake news were posted on the static news websites. Real and forged images were also used. Chatrooms and interactive platforms were used to generate favorable discussions. Hacks attacked and defaced government's websites to voice their dissent against Yugoslav and NATO aggression. With traditional being limited to access and cover the issues, images, texts, audio clips, video clips were used to harness emotions of fear, hate, and sympathy (Denning, 2001).

Igor Panarin is one of the contemporary architects of Russian military doctrines including reflexive control, and has sketched an outline of tools which can are used in contemporary information confrontation operations. The first instrument is propaganda which is further divided into three categories. The first category is white propaganda. In white propaganda, the origin or identity of the sponsor is known. The second category is grey propaganda. The identity of sponsor or origin is known. The purpose is to spread confusion and panic. The third category is black propaganda where the identity of the origin or sponsor is not known and public opinions are made to shift and change. The second instrument of information confrontation is intelligence. Information and communication technologies are used to gather specific information. The third instrument is analysis which includes monitoring geo-political landscape. This is done by monitoring and situation analysis. The last is the instrumentalization of communication technologies in organization and is achieved through the combination and integration of the aforementioned instruments when media is used to influence and shape desirable public opinion (Legucka, 2022). Panarin has also presented vehicles of influence operations. The first two vehicles are *social control* and *social maneuvering*. These are used to gain control over the collective behavior of a society. These vehicles are also helpful in acquiring power over people- politically, religiously, ideologically and cognitively (Darczewska, 2014).

In Ukrainian crisis of 2014, Russia is believed to use *Strategic Deception* as information operation in its foreign policy. *Strategic Deception* is not exactly a Russian military terminology. Nevertheless, it has always been a part of Russian military doctrine in essence in soviet ages as dezinformatsiya. However, the contemporary Russian *Strategic Deception* techniques are multifaceted. The use of propaganda and disinformation is evident in all operations. In addition to this, in the digital age with readily available information, cloaked content is easy to produce. Russia achieved informational goals through five strategic deception strategies. Firstly, it provided negative information about its adversaries and unfriendly countries. Negative information tends to have more acceptability among audiences than positive information. Secondly, it tried to influence the policies of Ukrainian and allies' governments through military deception, intimidation, and social maneuvering. Thirdly, with disinformation and propaganda aimed at maligning and discrediting political leadership Russia tried to undermine their authority. Fourthly, Russia tried to disrupt Ukraine's relations with other countries through imposter accounts, hate mongering content, use of intimidation, and building better relations with other countries. Fifthly, Strategic Deception also included weakening governmental and non-governmental organizations through discrediting them (Pynnöniemi & Rácz, 2016).

Research Methodology

The study has used qualitative research methodology. The integration of Information-Technical (IT) and Information-Psychological (IP) has been studied a single case in Pegasus Operations. The operation was selected for its global impact, cyber capabilities, and extensive evidence of itse use in surveillance and espionage. Additionally, the operation also reflects integration of both IT and IP. The paper has used data from sources including forensic reports, investigative reports, messages and content used in Pegasus. This has also ensured triangulation of data from multiple sources. Qualitative thematic analysis was used to identify themes, narrative patterns, psychological triggers and manipulation in messages used for Pegasus linked attacks.

Discussion and Anaylsis

The contemporary Information Operations are also divided into two categories. This categorization is done on the basis of their operation theatre which is as follow:

Information Technical

Information Technical is the tangible sphere of Information Operations. Operations in Information- Technical are called Cyber Attacks/Operations. These operations include attacking and protecting critical cyber and computer infrastructure. The offensive operations are conducted through hacking, espionage, infiltration and disruption of an adversary's critical cyber infrastructure, database, website or even official handles on social media. These attacks also include denial of internet and other services to citizens. Furthermore, attacking an adversary's computer networks, content and data bases of media organizations, financial institutions, educational institutions, non-governmental organizations, trade unions and associations, social advocacy and activist groups, opinion leaders, private targets, public discussion forums are included in Information-Technical. The subtle nature of Information-Technical Operations means that actions are non-attributable to one military or government. One such example of Information-Technical is 'Operation Armagedon' (mistakenly misspelled in official documents) launched in 2013 during Ukrainian crisis. The operation was launched through local hackers of Ukraine including CyberBerkut. Denial-of-service attacks were planned on Ukrainian government's official websites and webpages, and defaced the portals. The hackers also attacked NATO's websites and portals. The hackers were also successful in seizing US-Ukraine military coordination documents. Additionally, the group also tried to manipulate Ukrainian General Elections by attacking Election Commission website and databases.

Furthermore, camouflage and deception were also strategically used in the operation. In order to access and penetrate into the databases, bogus and imposter firms (example: Tramac) were established. Such firms were established in different countries. Dozens of real and imposter employees were hired. Media coverage was arranged for the activities of such companies. Government officials were targeted through emails and attachments.

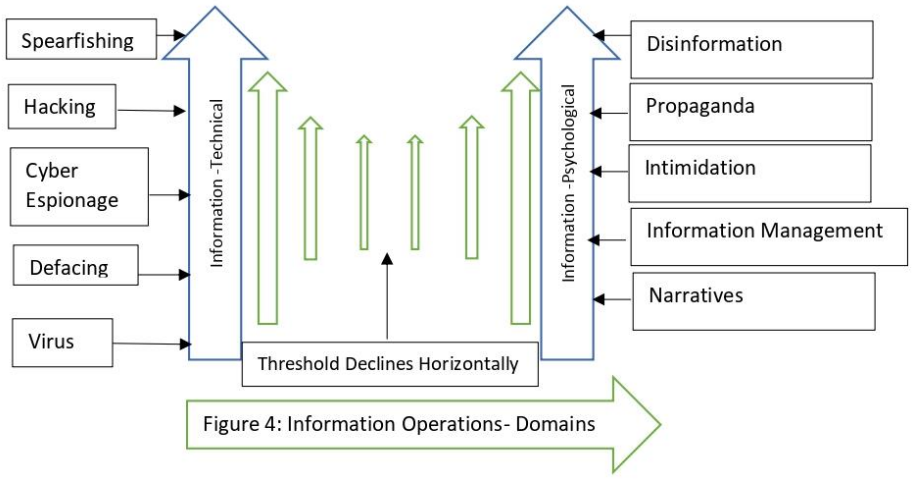
Interestingly, Operation Armageddon was detected through MS Office word file. Although, the operation is attributed to Russia. Nevertheless, no official acknowledgement exists from Russian side. Furthermore, owing to the elusive nature of the operation there was no bloodshed and therefore, Russia maintained minimum level troop deployment. All these led to the delayed global outcry.

Information-Psychological

Information-Psychological Operations are designed to target a desired population psychological. The operations include building narratives, propaganda campaigns through white, grey, and black, misinformation, disinformation, malinformation, lies, truths, half-truths, twisted facts, coercion, intimidation, greed etc. Information Psychological is also elusive and subtle in nature. The desired effects are achieved through liminal and subliminal messages. The use of lies and twisted facts is meant for domestic and foreign population. The information environment is saturated with disinformation and alternative facts. In order to counter an undesirable public discourse, *Information Pollution* technique is used. Mass and widespread creation and sharing of content does not only bury the information in public discourse but it also conceals critically information through diverting public discourse on other issues. The inculcation of desired opinions and narratives is achieved through over simplification of otherwise complex issues, repetition and reinforcement of ideas and ideologies, and massive content sharing and creation forces users to believe. At times, invigorating an old concept and exacerbating a new idea also question public perception of issues. In a state of confusion, public opinion is swayed by deploying public understanding in complexities. Moreover, Information-Psychological Operations are also planned for domestic audiences. Censorship and control of news is done to restrain undesirable ideas being floated in the public discourse. The use of opinion leaders and celebrities is another technique to sway public opinion in favor

(Iasiello, 2017). Georgia's Rose Revolution of 2003 is a good example in this regard. The peaceful transformation of power was the result of a well-organized political communication campaign. Public Relations Organizations and Management Firms were used by the opposition parties. The Rose Revolution is considered to be a failure of Russian Information Operations. During the crisis, Russian media and political leadership were found to be less aggressor than their Georgian counterpart. Georgian free media maintained political discussion on television against the Russian supported government. Western countries also supported opposing parties and their media organizations gave extensive coverage in favor of the opposition parties. Russian government could however, only control narrative domestically (Levine, 2008). It is important to discuss here that Russia had weak economy and lacked military fervor in 2003.

This is evident that Information Operations have been operationally used in two domains- Informational and Psychological. It can also be concluded on the basis of existing literature that Information Operations have been used in two domains under one operation as the following visualization depicts.



Integration of Information-Technical and Information-Psychological: A Case of Pegasus

Information-Technical and Information-Psychological have been conducted in parallel manner. The two categories have been constituents of single operation. Nevertheless, the two were rarely integrated in one single action. In contemporary Information Operations however, Information-Technical and Information-Psychological have been immersed into each other to maintain and enhance operational efficacy. One such case is of 'the Pegasus'. Niv, Shalev and Omri infamously known as the NSO group is an Israeli Cybersecurity, Cyber Surveillance, and Technology firm. The NSO Group developed and sold a hacking and cyber espionage software named 'Pegasus'.

The news about the spyware attracted global attention when an Arab journalist was blackmailed on the basis of data extracted from his phone. Upon conducting the forensics of the mobile phone by a Canadian firm, it was revealed that the phone was targeted through spearfishing and was infected with a very state of the art and sophisticated spyware. Further investigation revealed the structural and operational dynamics of the spyware. It was revealed that spyware was developed with an ability to remotely accessed features. The features of the software could turn on a device of its own. The functions which the spyware could remotely operate included extracting of stored data both physically and in cloud, camera, microphone, GPS, and all sensors available in the device. The spyware could perform several functions including downloading and sending contact details, images, passwords, messages, emails, record and send phone calls audios, take and send pictures, videos. The spyware easily converted mobile phone and other devices into twenty-four hours surveillance devices (Bazaliy,

et al., 2016). More interestingly, it is argued that unlike other spywares, Pegasus was advanced to zero-click attacks meaning it required no apparent activity by the victim. Nevertheless, the zero-click attack capability of Pegasus remains debated. A report by EU estimated that as of 2021 Pegasus operators could be conducting cyber operations in 45 countries (Marzocchi & Mazzini, 2022).

It is commonly believed that several social and digital media apps, emailing and messaging apps are encrypted. However, once spearfished, Pegasus could access data from approximately all such apps including Google, Gmail, Yahoo, WhatsApp, WeChat, Safari, Skype, Facebook, Facetime etc., (Bazaliy, et al., 2016). NSO Group leadership maintained that the Pegasus was built and used for vetted government clients to be used against criminals and non-state actors. The group leadership also denied any activity of cyber espionage being conducted through Pegasus against any head of the state or government or person of interest not related to terrorism or crime (Marzocchi & Mazzini, 2022).

Pegasus was not only used in cyber surveillance and espionage by different governments internally but it was also used externally. Governments and intelligence organizations used Pegasus for espionage against their politicians, famous persons, journalists, activists, and other civil society members. The Pegasus was also used for surveillance of non-state actors. Governments and intelligence agencies also used Pegasus against governments, politicians, military leadership, journalists, opinion leaders from their rival/enemy countries. It has been reported that Pegasus was used in series of attacks by operators in Pakistan as well. Amnesty International with 17 media groups formed a team called 'Project Pegasus' to investigate and probe Pegasus operations. The findings of the investigation were shocking for countries, tech giants, civil society, and governments. A total of fourteen of head of the governments and head of the states were targeted/victimized through Pegasus attacks (Marczak, Scott-Railton, McKune, Razzak, & Deibert, 2018). These leaders included former Pakistani Prime Imran Khan and French President Emanuel Macron. The publisher of the report is the same lab that first detected Pegasus in a mobile phone of an Arab journalist.

Pegasus is a spyware used for hacking, espionage, data stealing, surveillance and remote operations. The nature and structure of Pegasus falls into the category of Information-Technical. Nevertheless, the way Pegasus attacks were mostly executed falls into the category of Information-Psychological. Marczak et al. (2018) investigated the links and domains which were used in the Pegasus attacks in 45 countries. The findings about Pakistan indicate the operator of Pegasus attacks in Pakistan was 'Ganges'. The same operator also targeted persons of interests in Bangladesh, Brazil, Hongkong, and India. The theme on which the domain was 'Political' in nature. The domain which was used in attacks in Pakistan was "*signpetition[.]co*". The selection of the theme is important because in many of the Pegasus attacks an action was required by a victim that might be a click, download, or a tap. The use of political theme indicates that users can be motivated to an action on the basis of their interest in politics or political opinions. The cited report was a track of Pegasus from 2017 to 2018. Amnesty International published a report in 2021. The report indicates the Information-Psychological element of Pegasus. Former Indian Delhi University Professor Syed Abdul Rehman Geelani was a victim of series of attacks from February 2018 to October 2019 (Amnesty International , 2021). The links which were used to spearfished the user indicate that political themes were used. The victim's cognitive interests were motivational factors to open the links. The links were created as news stories. Headlines and captions baited the user to open the links. The first link that the victim received in February 2018 was in a SMS and the caption said, "United Nations launches online portal for the independence of Kashmir. To cast your online vote, click here http://bit[.]ly/2o487h1 (https://signpetition[.]co/vU1zwaqFh)".

The clickbait enticed victim to take a political action. The message clearly indicates that the victim possessed cognitive interest in Kashmir Issue, and favored Pakistan's narrative about Kashmir. Furthermore, the evidence also supports the findings of Marczak et al (2018) as the domain which was used in this message was

same as in their report. The comparative analysis of both the reports clarifies things. Evidence suggests that the victim preferred political content related to Kashmir. The domain was also same-indicating that the operator was "Ganges" who operated in Pakistan, Bangladesh, India, Hongkong, and Brazil.

Four days later, SAR Geelani received another SMS from the same number that said, "BJP hatches conspiracy for a Muslim free Jammu region through medical poisoning of Muslims. http://bit[.]ly/2o95TNh (http(space)s://news-alert[.] org/TfteZB6wK)." This message was also about Kashmir. However, this time the content was about Muslims in Kashmir and anti-BJP narrative was embedded in the content.

A day later, the victim received another message from the same number that said, "Another incident showing Indian army beating librandu Kashmiri youth mercilessly to chant Pakistan Murdabad. http://bit[.]ly/2ob9QkO (https://news-alert[.]org/K9pAkFk3R)." The theme was based on Kashmir issue that can be categorized as political. The link was disguised as a news story. The difference in this message was about 'Indian forces committing atrocities' in Kashmir. The text indicates the victim's interest in Kashmir unrest and 'atrocities' by Indian forces on Kashmiri youth.

The victim did not receive any other message for the next two months. In April 2018, an SMS came from the same number that said, "Organization of Islamic countries (OIC) launches online portal for the independence of Kashmir from India. For the detailed article, click here http://bit[.]ly/2Hk1UJE (https://newsalert[.]org/WW7G1EW2)." A day later, the victim received another SMS from the same number that said, "Global powers urge Indian leadership to concede the entire Jammu & Kashmir to Pakistan for regional peace and stability. For the detailed article, click here. https://news-alert[.]org/T1q4YjItT."

Interestingly, the timeline of these attacks was parallel to the killings of twenty individuals in Jammu and Kashmir in April 2018. The theme was political. The sentiment was Pro Kashmir Movement, Pro-Pakistan.

Three days later, same number sent another message. However, the theme of this message was totally different. The SMS said "Hot & sexy male & female escorts available at 60% discount. To avail the service, please click on https://myprivacy[.]co/Ooboe7u." This time the theme was sexual.

Next day, the victim received a new SMS from the same number. The message said "European Union leads its unconditional support to India over the issue of Kashmir during the current visit of PM Modi. For more details, click https://my-privacy[.]co/j2xgK558." The theme of the message is political. The message invokes political insecurity in the victim.

The next message that the victim received said "India & America strategically conspiring for the failure of China Pakistan Economic Corridor (CPEC). For the detailed article, click here. https://my-privacy[.]co/ZOubFbXW." This message also carries political theme. However, unlike previous message, this message was about China Pakistan Economic Corridor. The message also seems to invoke political insecurity in the victim's mind. The sentiment is Anti-India and Anti-America, and Pro-Pakistan.

Few days later, the victim received a news SMS that said "Pakistan in all probability will become the next province of China through China Pakistan Economic Corridor (CPEC)." The message carries political theme. The sentiments were anti-CPEC and Anti-India.

Figure 1 Visualization of most frequent words used in the messages designed by the researcher

Pegasus attacks and operations explain that in order to achieve desirable action from a target, individual's profile, cognitive interests, cognitive biases, political inclinations and association, religion, education, existing beliefs and opinions can play a very detrimental role. An advisory by the Government of Pakistan among other highlighted "Social Engineering" in Pegasus Attacks (Government of Pakistan, 2021). Social Engineering is also defined as human hacking. Hackers, criminals all across the globe use social engineering tactics to phish and hack. Hacking is seen a purely technologically oriented and falls in the category of Information-Technical. Pegasus used social engineering to entice victims to take a certain action. The planned action could amplify hacking and cyber espionage operations. Social Engineering can be defined as planned activities aiming at cognitively manipulating an individual. It also includes exploitation of existing cognitive biases. Emotional exploitation is also done in social engineering. According to the united Kingdom's national Computer Emergency Response Team (CERT), the most the common social engineering attacks are "Phishing" and "Baiting" (CERT-UK, 2015). Both categories of attacks are planned psychologically and carried out technologically in the age of social media.

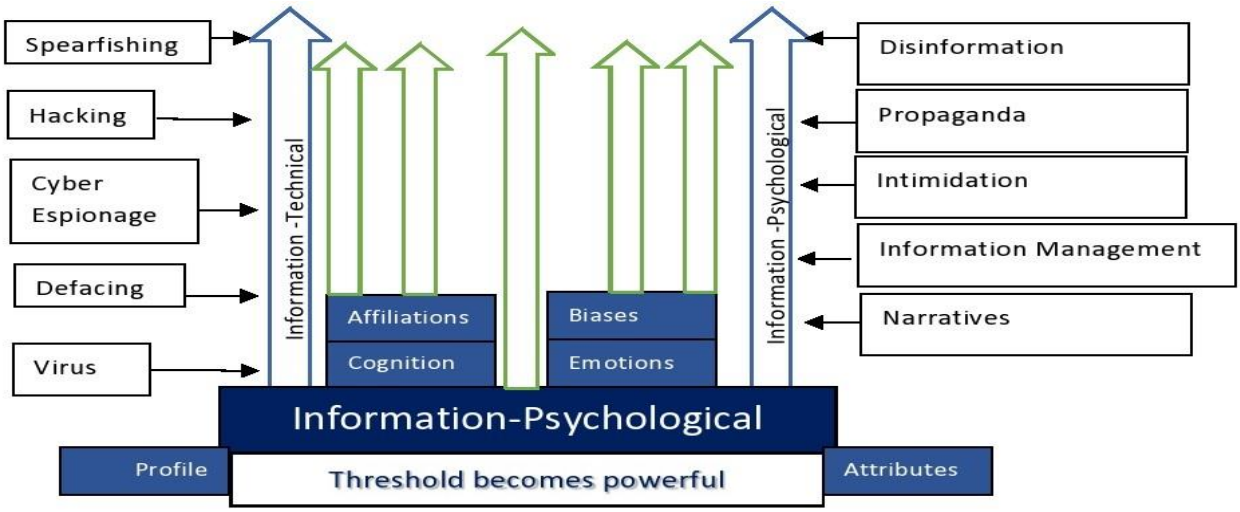


Figure 2 Integration of I-T and I-P- designed by the researcher of this study

Figure 3 shows that with the integration of Information-Technical and Information-Psychological information operations become more powerful. It is argued the most enduring weapons are cognitive weapons because their destruction is long lasting. In this information age, human cognition has become target and social media has been weaponized.

US (DoD, 2014) categorizes information operations into Information-Technical and Information-Psychological. While studying operations and activities of "Operation Armageddon" in which both spheres were used as Area of Operations. However, while studying "Pegasus" of the NSO group. It can be argued that contemporary information operations become lethal when Information-Technical and Information-Psychological spheres are immersed.

Conclusion

This study has shown that there is a transition in cyber operations and psychological operations. Contemporary information operations are increasingly integrating the two categories into an integrated operational framework. The Pegasus spyware example explains how cyber espionage can be effectively combined with social engineering, behavioral profiling, emotional exploitation, and politically crafted messages to achieve maximum operational effectiveness. The results also show that cyber operations today are not limited to the hacking of devices or stealing of information. These are aimed at influencing how people perceive, behave, and make decisions in the cognitive environment. The convergence of cyber and psychological operations acts as a force multiplier when conducting fifth generation hybrid conflicts. As information and communication technologies continue to have a major influence on political, social and strategic issues, state and intelligence agencies are likely to further develop institutionalized capabilities

References

Amnesty International . (2021). Forensic Methodology Report: How to catch Pegasus. London : Amnesty International.

ATP. (2018, October 4). The Conduct of Information Operations. Retrieved from Army Publication Directorate: https://atiam.train.army.mil/catalog/dashboard

Bazaliy, M., Hardy, S., Flossman, M., Edwards, K., Blaich, A., & Murray, M. (2016). Technical Analysis of Pegasus Spyware: An Investigation Into Highly Sophisticated Espionage Software. San Francisco : Lookout.

CERT-UK. (2015). An Introduction to Social Engineering. London: Computer Emergency Response Team (CERT-UK).

Darczewska, J. (2014). The Anatomy of Russian Information Warfare: The Crimean Operation- A Case Study. Warsaw: Ośrodek Studiów Wschodnich.

Denning, D. E. (2001). ACTIVIM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING FOREIGN POLICY. In J. Arquilla, & D. R. (Eds), Networks and Netwars: The Future of Terror, Crime, and Militancy (pp. 239-288). Santa Monica: RAND Corporation .

DoD. (2013, 5 2). Information Operations. Retrieved from US Department of Defense .

DoD. (2014, 11 20). Information Operations . Retrieved from Homeland Security Digital Library : https://www.hsdl.org/?abstract&did=759867

Giles, K., Sherr, J., House, C., & Seaboyer, A. (2018). Russian Reflexive Control. Kingston: Royal Military College Canada .

Government of Pakistan. (2021, July 30). Cyber Security Advisory- Pegasus Cyber Espionage and Intelligence Tool of NSO Group. Islamabad, Pakistan.

Grčar, M., Cherepnalkoski, D., Mozetič, I., & Novak, P. K. (2017). Stance and influence of Twitter users regarding the Brexit referendum. Computational Social Network, 1-25.

Iasiello, E. J. (2017). Russia's Improved Information Operations: From Georgia to Crimea. Parameters, 51-63.

Johnson, R. (2017). The Evolution of Hybrid Threats Through History. In Y. Ozel, & E. Inaltekin, Shifting Paradigm of War: Hybrid War (pp. 1-3). Istanbul: Turkey National defence University Printing House.

Keenan, T. (2001). Looking Like Flames and Falling Like Stars: Kosovo, 'the First Internet War'. Social Identities , 539-550.

Korypko, A. (2015). Hybrid Wars: The Indirect Adaptive Approach to Regime Change. Moscow: People's Friendship University of Russia.

Legucka, A. (2022). RUSSIAN DISINFORMATION: OLD TACTICS-NEW NARRATIVES. In A. Legucka, & R. Kupiecki, Disinformation, Narratives and Memory Politics in Russia and Belarus. Oxon: Routledge .

Levine, Y. (2008, August 13). The Cnn Effect: Georgia Schools Russia in Information Warfare. Retrieved from The Exiled : http://exiledonline.com/the-cnn-effect-georgia-schools-russia-in-information-warfare/

Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A., & Deibert, R. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries . Toronto : Citizen Lab.

Marzocchi, O., & Mazzini, M. (2022). Pegasus and Surveillance Software. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs European Parliament.

Pynnöniemi, K. P., & Rácz, A. (2016). Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine. Helsinki: The Finnish Institute of International Affairs.

Roberts, J. Q. (2015). Maskirovka 2.0: Hybrid Threats, Hybrid Response . McDill: Joint Special Operations University Press.

Thomas, T. L. (2004). Russia's Reflexive Control Theory and Military . Journal of Slavic Military Studies, 237-256.

Thomas, W. I., & Thomas, D. S. (1928). The child in America. Knopf: Oxford.

US DoD. (2011). Information Operations Primer. Carlisle Barracks: US Army War College.

US TRADOC. (2016, June 13). Retrieved from US Department of Defense : https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

Zaighum, Z., & Rasool, F. (2023). Fifth-Generation Hybrid Warfare in Pakistan: Mapping Hybrid Threats, State Interpretation, and the Way Forward. IPRI Journal, 53-79. doi:DOI: 10.31945/iprij.230103