BIPSS Commentary
www.bipss.org.bd
January - 2025
BIPSS Towards a Secure World

Information Warfare: A battlefield without bullets

Shamshil Arefin[1]

Introduction

Information warfare (IW) refers to the strategic use and management of information and communication technology to gain a competitive advantage over adversaries. It encompasses a range of activities aimed at manipulating, disrupting, or controlling information to influence decision-making processes in favor of the initiator.[2] This form of warfare has evolved significantly with advancements in technology, making it a critical component in modern military and political strategies. Information warfare involves the acquisition, manipulation, and dissemination of information to influence decision-making, disrupt operations, or gain strategic advantages. It often targets human psychology, communication systems, and technological infrastructure. Information warfare can be defined as operations conducted to achieve information superiority by affecting adversary information systems while protecting one's own. This includes not only the offensive actions against an opponent's information capabilities but also defensive measures to safeguard one's own systems from similar attacks.

Components of Information Warfare

The scope of information warfare is broad and can include various forms such as:

Cyber Warfare

Cyberwarfare entails the carrying out of defensive and offensive operations in the cyberspace domain. Such operations focus on computer systems and networks to disrupt operations or steal

[1] Shamshil Arefin is currently a Research Assistant at Bangladesh Institute for Peace and Security Studies (BIPSS). He has completed his BSS in International Relations from Bangladesh University of Professionals (BUP).

[2] Lawrence Freedman, "Information Warfare," The Revolution in Strategic Affairs, October 28, 2020, 49–64, https://doi.org/10.4324/9781315000886-5.

sensitive data. It can refer to the use of digital attacks by one nation-state against another to disrupt, damage, or destroy critical systems and infrastructure. These attacks can target government operations, military assets, financial systems, and essential services, aiming to compromise national security and cause widespread disruption. The usage of advanced technologies such as malware, ransomware, and Distributed Denial of Service (DDoS) are signature tools used in cyber warfare. Any mechanisms or tools that is used to harm the digital communications.[3]

Psychological Warfare

Psychological warfare (psywar) is a crucial aspect of information warfare that focuses on the planned use of propaganda and psychological operations to influence the opinions, emotions, and behaviors of target audiences. This strategy aims to demoralize opponents, manipulate perceptions, and ultimately achieve strategic objectives without necessarily resorting to physical combat.[4]

Psychological warfare employs various methods and techniques designed to influence target populations, including propaganda, demoralization, disinformation, and psychological operations (PsyOps). Propaganda involves the dissemination of carefully crafted messages through different media channels to shape perceptions, categorized into white (truthful information), black (false information), and gray (ambiguous information), each serving purposes such as promoting ideologies or discrediting opponents. Demoralization tactics aim to undermine the morale of enemy forces by distributing leaflets encouraging desertion or using loudspeakers to broadcast messages of defeat, creating doubt and fear among enemy troops and reducing their will to fight.[5] Disinformation involves deliberately spreading false information, such as fake news stories, manipulated images, or staged events, to mislead adversaries, create confusion, and disrupt

[3] Aro, J. (2016), The Cyberspace War: Propaganda and Trolling as Warfare Tools, European View, (15), 121–132.

[4] Galih Adi Putra, Muhammad Hadianto Wirajuda, and Helda Risman, “Psychological Warfare as a Driving Factor in the Development of Military Strategy during the Gulf War 1990-1991,” *Advances in Social Sciences Research Journal* 11, no. 1 (January 18, 2024): 97–106, https://doi.org/10.14738/assrj.111.16262.

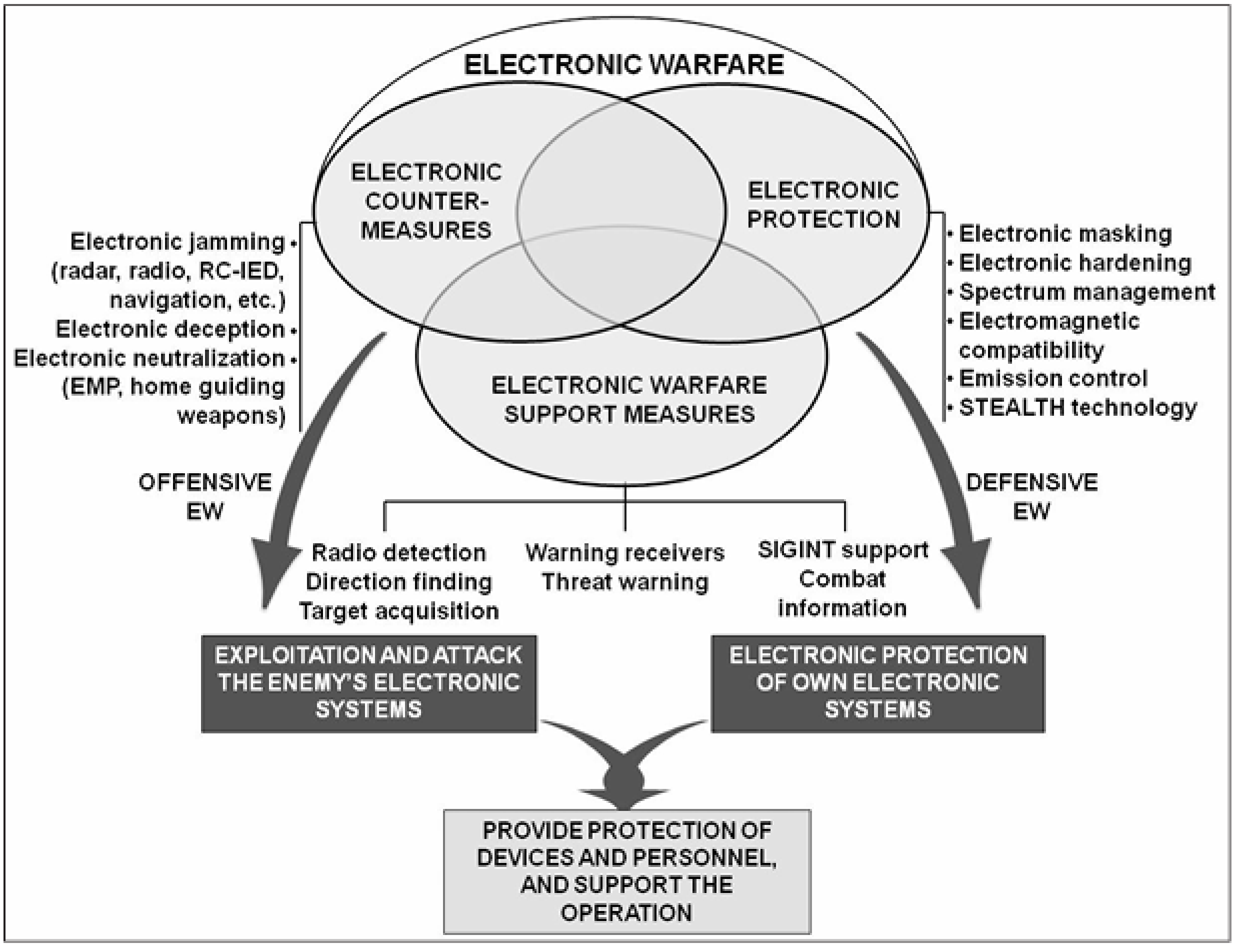
[5] United Nations Office on Drugs and Crime, “Cybercrime Module 14 Key Issues: Information Warfare, Disinformation and Electoral Fraud,” www.unodc.org, June 2019, https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html.

decision-making processes. PsyOps are organized campaigns targeting specific demographics with messages intended to incite action or inhibit resistance, such as the Gulf War radio broadcasts encouraging Iraqi soldiers to surrender.

Electronic Warfare

Electronic warfare (EW) is a critical component of information warfare that utilizes the electromagnetic spectrum to achieve military objectives. It encompasses a range of operations designed to exploit, disrupt, or deny enemy use of electronic systems while ensuring the protection and effectiveness of friendly forces. The strategic use of EW has become increasingly important in modern conflicts, where information dominance can significantly influence the outcome of military engagements[6].

[6] Encyclopaedia Britannica, "Electronic Warfare," www.britannica.com, June 22, 2016, https://www.britannica.com/topic/electronic-warfare.

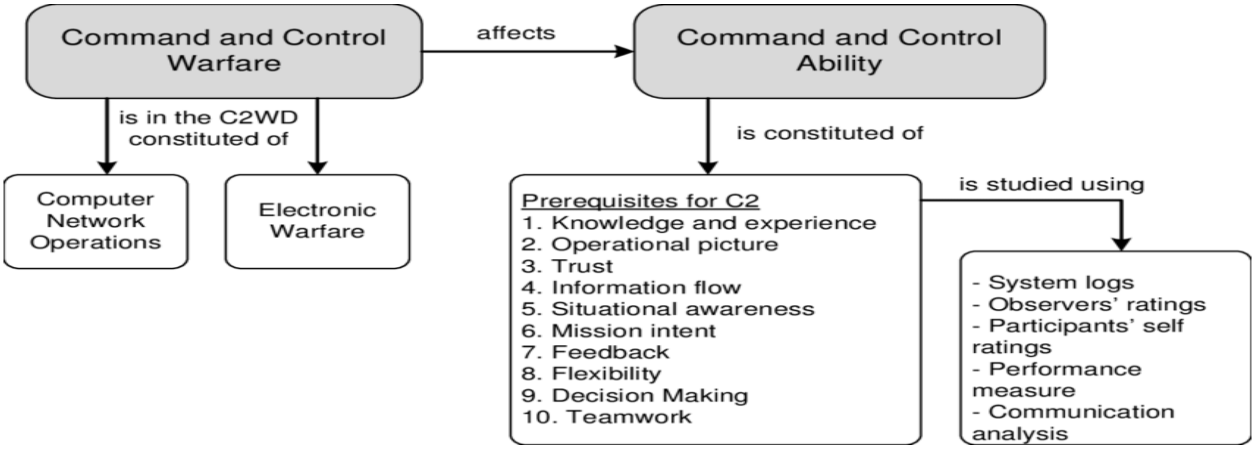

ELECTRONIC WARFARE
ELECTRONIC COUNTER-MEASURES
ELECTRONIC PROTECTION
ELECTRONIC WARFARE SUPPORT MEASURES
Electronic jamming • (radar, radio, RC-IED, navigation, etc.)
Electronic deception •
Electronic neutralization • (EMP, home guiding weapons)
• Electronic masking
• Electronic hardening
• Spectrum management
• Electromagnetic compatibility
• Emission control
• STEALTH technology
OFFENSIVE EW
DEFENSIVE EW
Radio detection
Direction finding
Target acquisition
Warning receivers
Threat warning
SIGINT support
Combat information
EXPLOITATION AND ATTACK THE ENEMY'S ELECTRONIC SYSTEMS
ELECTRONIC PROTECTION OF OWN ELECTRONIC SYSTEMS
PROVIDE PROTECTION OF DEVICES AND PERSONNEL, AND SUPPORT THE OPERATION

Source: Haig, 2015

Electronic warfare is typically divided into three main components: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES), each playing a distinct role in military operations. Electronic Attack (EA) involves offensive measures aimed at disrupting or degrading enemy electronic systems, using techniques like jamming, which floods enemy communications or radar with noise to prevent effective operation, and spoofing, which sends false signals to mislead adversaries about the location or nature of friendly forces. EA also includes the use of directed energy weapons and anti-radiation missiles that target enemy radar or communication signals to neutralize them, providing friendly forces with a tactical advantage by blinding or confusing enemy systems. Electronic Protection (EP) encompasses defensive measures to safeguard friendly electronic systems from enemy attacks, such as frequency hopping, which rapidly changes transmission frequencies to evade jamming, and emission control (EMCON), which limits electronic emissions to reduce detection risk. EP ensures critical communication and navigation systems remain operational in contested environments, allowing for continued coordination and effectiveness during operations. Electronic Warfare Support (ES) focuses on gathering intelligence on enemy electronic systems by intercepting communications and identifying radar emissions to gain insights into their capabilities and intentions. The intelligence gathered through ES is essential for planning effective EA and EP strategies, enhancing situational awareness and informing decision-making processes.[7]

Command and Control Warfare

Command and Control Warfare (C2W) is a military strategy that focuses on disrupting and degrading the command and control (C2) capabilities of adversaries while protecting those of friendly forces. It encompasses a range of tactics and techniques aimed at influencing the decision-making processes of enemy commanders, thereby gaining a strategic advantage in military operations. C2W integrates various elements of information warfare, including electronic warfare, psychological operations, military deception, operations security, and physical destruction.[8]



Source: Granasen, Magdalena & Lif, Patrik & Oskarsson, Per-Anders & Klum, Peter & Tydén, Lars & Hallberg, Niklas. (2011)

[7] Zsolt HAIG, "ELECTRONIC WARFARE in CYBERSPACE," *Security and Defence Quarterly* 7, no. 2 (June 30, 2015): 22–35, https://doi.org/10.5604/23008741.1189275.

[8] Dan Struble, "What Is Command and Control Warfare?," *Naval War College Review* 48, no. 3 (1995): 89–98, https://doi.org/10.2307/44642810.

The primary objective of C2W is to undermine the adversary's ability to effectively command and control their forces. This is achieved by targeting the flow of information between enemy units and their command structures. By disrupting this communication, C2W aims to create confusion and uncertainty within enemy ranks, forcing them to react to situations rather than proactively plan their operations.[9] This reactive posture can lead to mistakes, miscalculations, and ultimately, a loss of initiative in combat scenarios.

The Blurred Lines Between War and Peace

Although the term ‘information warfare’ presumes that actors are engaged in open conflict, the reality is often not as straight-cut as we may believe. Several instances which are used as examples of information warfare did not necessarily cause warfare as these actions alone often do not meet the threshold for conventional warfare. This anonymity complicates responses from traditional military forces and law enforcement agencies. As a result, actors tend to develop animosity against one another which deteriorates as information warfare rages on. Such negative interaction can cause this latent hatred to spill over into open violence and conflict due to other complementary factors. Information warfare tends to attack the psyche of the general populace rather than any physical installations or resources. This is obtained through the spread of misinformation and propaganda creating chaos and uncertainty.[10] One of the main reasons for engaging in information warfare is to impact the policy making apparatus through disheartening the populace and organizing discord. This psychological manipulation can have the desired goal of creating chaos without risking physical confrontation.

[9] Martin Hristov, “Points of Intersection and Dependencies Between Information Operations And Command And Control Warfare,” (The 16th International Scientific Conference Strategies XXI” Technologies – Military Applications, Simulation And Resources, 2020).

[10] Nazish Mahmood, Ahmed Ijaz Malik, and Muhammad Nadeem Mirza, “Analysing Hybrid Warfare and Information/Cyber Operations,” *Webology* 18, no. 4 (August 15, 2021): 1720–31, https://shs.hal.science/halshs-03788137.

Source: Science Friday

The rapid dissemination of information in the digital age significantly enhances the effectiveness of information warfare, as false narratives can spread quickly through social media and other online platforms, making it challenging for governments and organizations to counteract misinformation before it takes hold in public consciousness. This speed of information spread can lead to swift changes in public opinion or political landscapes, as disinformation can reach vast audiences almost instantaneously. The ease with which information can be shared online means that disinformation campaigns can exploit this rapid flow, creating confusion and mistrust among the populace. Furthermore, the complexity of attribution presents another layer of danger in information warfare; identifying the source of attacks—such as cyber intrusions or disinformation campaigns—is often difficult due to the anonymity provided by digital platforms. This difficulty complicates responses and may prevent targeted nations from retaliating effectively against aggressors, as the lack of clear accountability emboldens adversaries to engage in information warfare tactics with reduced fear of repercussions.[11] Consequently, the combination of rapid dissemination and complex attribution creates a volatile environment where misinformation can thrive and undermine societal trust, making information warfare a potent and dangerous tool in contemporary conflicts.

Challenges of Digital Anonymity

The anonymity provided by digital platforms significantly complicates the attribution of information warfare attacks, such as cyber intrusions and disinformation campaigns. This challenge arises from several factors inherent to the nature of cyberspace. The architecture of the Internet allows cyber attackers to mask their identities, making it difficult to trace malicious activities back to specific individuals or groups. Techniques such as IP spoofing enable attackers to conceal their true origin by using fake addresses, further obfuscating their identity and complicating the identification process. The use of anonymizing tools, such as Virtual Private Networks (VPNs) and Tor networks, allows perpetrators to conduct operations without revealing their location or identity, creating a layer of plausible deniability. Obtaining physical access to a perpetrator's computer or network can be challenging due to the need for international cooperation, as jurisdiction, varying state laws, and the effectiveness of nation’s law enforcement agency create another layer of complexity that needs to be navigated. The complexity is further heightened by the potential for state-sponsored attacks where data may be doctored or fabricated to mislead investigators about the true source of an attack.[12]

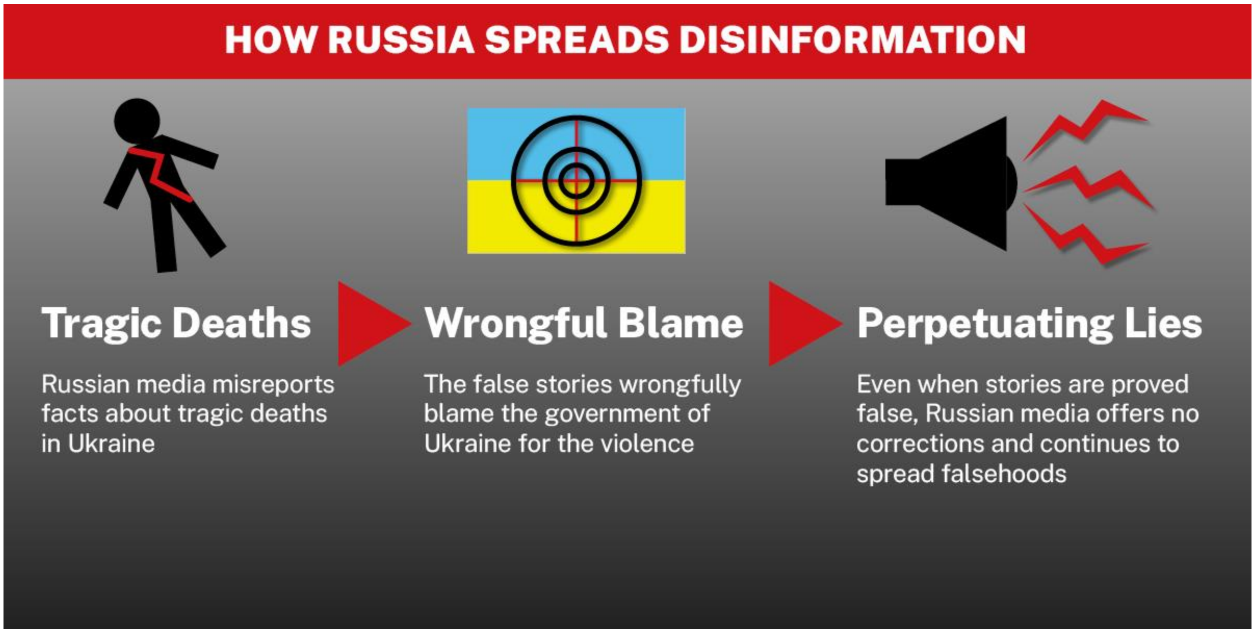
The Russian Disinformation Campaign

The ongoing conflict between Russia and Ukraine serves as a contemporary and illustrative example of information warfare's multifaceted nature and its profound implications on geopolitical dynamics. Following Russia's annexation of Crimea in 2014, the Kremlin employed a

[11] Waseem Ahmad Qureshi, “Information Warfare, International Law, and the Changing Battlefield,” *Fordham International Law Journal* 43, no. 4 (2020), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2786&context=ilj.

[12] Glenn Voelz and Sarah Soliman, “Identity, Attribution, and the Challenge of Targeting in the Cyberdomain,” *MCU Journal* 7, no. 1 (April 8, 2016): 9–29, https://doi.org/10.21140/mcuj.2016070101.

comprehensive strategy that integrated cyber operations, disinformation campaigns, and psychological tactics to achieve its political objectives. This approach has often been described as a "test bed" for Russia's cyber capabilities, particularly since the EuroMaidan protests in 2013, which marked a pivotal moment in Ukraine's political landscape.[13]



HOW RUSSIA SPREADS DISINFORMATION

Tragic Deaths

Russian media misreports facts about tragic deaths in Ukraine

Wrongful Blame

The false stories wrongfully blame the government of Ukraine for the violence

Perpetuating Lies

Even when stories are proved false, Russian media offers no corrections and continues to spread falsehoods

Source: US Embassy in Georgia

One of the primary tactics utilized by Russia has been the dissemination of disinformation narratives aimed at justifying its military actions. For instance, Russian state media propagated the false narrative that the Ukrainian government was committing atrocities against Russian-speaking populations, portraying it as a legitimate response to protect these communities from alleged threats. This narrative was further reinforced by claims of Ukrainian nationalism being akin to Nazism, which served to legitimize Russia's intervention in the eyes of both domestic and international audiences.[14]

[13] Digital Forensic Research Lab, “Undermining Ukraine: How Russia Widened Its Global Information War in 2023,” Atlantic Council, February 29, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.

[14] Göran Bolin and Per Ståhlberg, “From Nation Branding to Information Warfare: Management of Information in the Ukraine-Russia Conflict,” academia.edu, 2016,

In addition to these narrative strategies, Russia has employed cyber warfare techniques to disrupt Ukrainian communications and sow confusion among military ranks. Reports indicate that Russian forces utilized various cyber tools, including Distributed Denial of Service (DDoS) attacks and spear-phishing campaigns, to target critical infrastructure and government communications. Notably, during the 2014 elections in Ukraine, Russian hackers attempted to manipulate election results by undermining public trust in the electoral process.[15]

The use of social media platforms has been integral to Russia's information warfare strategy. The Kremlin has deployed coordinated disinformation campaigns across social media channels to amplify its narratives and create divisions within Ukrainian society. This tactic not only targets Ukrainian citizens but also aims to influence public opinion in Western countries regarding their support for Ukraine. The effectiveness of these operations is underscored by their ability to create uncertainty and undermine trust in democratic institutions.[16]

The implications of these information warfare strategies are profound; they have not only shaped military engagements but have also altered geopolitical dynamics in the region. The confusion and misdirection caused by Russian information operations had delayed western decision-makers, delaying effective responses to aggression. This highlights how information warfare can serve modern conflicts, which allows to be capable of achieving strategic objectives without traditional military confrontations.

https://www.academia.edu/28548429/From_Nation_Branding_to_Information_Warfare_Management_of_Information_in_the_Ukraine_Russia_Conflict?sm=b.

[15] Asma Rashid, Anum Yar Khan, and Syed Wasif Azim, “Cyber Hegemony and Information Warfare: A Case of Russia,” *Liberal Arts and Social Sciences International Journal (LASSIJ)* 5, no. 1 (June 30, 2021): 648–66, https://doi.org/10.47264/idea.lassij/5.1.42.

[16] Elina Treyger, Joe Cheravitch, and Raphael S. Cohen, “Russian Disinformation Efforts on Social Media,” www.rand.org (RAND, June 7, 2022), https://www.rand.org/pubs/research_reports/RR4373z2.html.

Conclusion

Information warfare has emerged as a powerful tool in modern conflicts, blurring the lines between traditional warfare and digital manipulation. This study has demonstrated that IW encompasses multiple dimensions, including cyber warfare, psychological operations, electronic warfare, and command and control warfare, each serving strategic functions in military and political engagements. The case of Russian disinformation campaigns highlights the potency of IW in shaping public perception, influencing policymaking, and destabilizing adversaries without direct military confrontation.

As the landscape of conflict continues to evolve, information warfare will remain a critical component of national security and global politics. Nations must adapt to this reality by developing comprehensive strategies that not only defend against adversarial information operations but also proactively engage in shaping and protecting their own information environments. Without such measures, the ability to maintain sovereignty, democratic integrity, and global stability will be increasingly compromised in an era where battles are fought not only with bullets but also with narratives and digital influence.