ARTICLE

INFORMATION WARFARE, INTERNATIONAL LAW, AND THE CHANGING BATTLEFIELD

Dr. Waseem Ahmad Qureshi[*]

ABSTRACT

The advancement of technology in the contemporary era has facilitated the emergence of information warfare, which includes the deployment of information as a weapon against an adversary. This is done using a number of tactics such as the use of media and social media to spread propaganda and disinformation against an adversary as well as the adoption of software hacking techniques to spread viruses and malware into the strategically important computer systems of an adversary either to steal confidential data or to damage the adversary's security system. Due to the intangible nature of the damage caused by the information warfare operations, it becomes challenging for international law to regulate the information warfare operations. The unregulated nature of information operations allows information warfare to be used effectively by states and nonstate actors to gain advantage over their adversaries. Information warfare also enhances the lethality of hybrid warfare. Therefore, it is the need of the hour to arrange a new convention or devise a new set of rules to regulate the sphere of information warfare to avert the potential damage that it can cause to international peace and security.

* Advocate Supreme Court of Pakistan.

I. INTRODUCTION

Information warfare is a combination of multifarious strategies aimed at harming the reputation or informational infrastructure of an adversary.[1] This tactic can be employed in times of both peace and war.[2] In particular, the information warfare strategy is relied upon widely by the actors of hybrid warfare.[3] States and nonstate actors involved in waging hybrid warfare employ information warfare tactics either to demonize their adversary by spreading disinformation, fake news, and propaganda or to harm the online security protocols of their adversary.[4] For instance, surreptitious and sudden online attacks on an adversary's cyberspace via hacking, the stealing of an adversary's confidential data adversary, or the deployment of social media campaigns to spread rumors against the adversary are some of the various tactics pursued within the sphere of information warfare.[5] In short, information warriors rely on using information as a precursor to causing intangible damage to the adversary.[6] The intangible damage can, sometimes, also bring tangible damage with it. For instance a virus attack on the command and control systems of an enemy's jet fighters can hinder

1. *See* LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 1 (1998).

2. VINCENT F. HENDRICKS & MADS VESTERGAARD, REALITY LOST: MARKETS OF ATTENTION, MISINFORMATION AND MANIPULATION 69 (2018).

3. *See, e.g.,* Przemyslaw Furgacz, *Russian Information War in the Ukrainian Conflict, in* COUNTERING HYBRID THREATS: LESSONS LEARNED FROM UKRAINE 207 (Niculae Iancu et al. eds., 2016).

4. *See id*. *See also* Cristian Barna, *The Road to Jihad in Syria: Using SOCMINT to Counter the Radicalization of Muslim Youth in Romania*, *in* COUNTERING RADICALISATION AND VIOLENT EXTREMISM AMONG YOUTH TO PREVENT TERRORISM 193 (Marco Lombardi et al. eds., 2015).

5. GREENBERG ET AL., *supra* note 1, at 1.

6. Alexander Nitu, *International Legal Issues and Approaches Regarding Information Warfare*, *in* PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY 201 (2011).

pilots in controlling planes, which can result in crashes and possibly causing human casualties.[7] In such an event, the law of armed conflict would be applied as the nature of the damage has turned from intangible to tangible.[8] On the other hand, when the impact of information operations is intangible damage, there are challenges in regulating information warfare under the authority of international law.[9]

Additionally, the right to freedom of opinion and expression, the common heritage of mankind ("CHM") principle, and the provisions of the Outer Space Treaty create restrictions for international law in regulating the operations of information warfare.[10] These restrictions make it difficult to legally bring information warfare within the regulation of the norms, rules, and principles of international law.[11] Consequently, information operations become unrestricted in their scope and functioning, which poses risks to international peace and security. This is because a lack of regulation can make the use of information warfare strategies uncontrolled, inviting rival states to use them against each other unrestrictedly.[12] The risks to peace and security deepen when information operations are installed by militant terrorists and anti-state actors.[13] Therefore, it is essential that the international community unites to legislate new rules regulating the conduct of states and nonstate actors whenever they use the strategies and tools of information warfare against any state or entity. The underlying challenges in doing so can be met through arranging a new convention on the issue and holding dialogues

---

7. E.g., Michael J. Robbat, *Resolving the Legal Issues Concerning the use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm*, 6 B. U. J. SCI & TECH. L. 26 (2000).

8. *Id.* at 13.

9. *See, e.g.,* GREENBERG ET AL., *supra* note 1, at 4. *See also* Phillip A. Johnson, *Is it Time for a Treaty on Information Warfare?, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 439 (Michael N. Schmitt & Brian T. O'Donnell eds., 2010).

10. *Id*.

11. Johnson, *supra* note 9, at 445-46.

12. Nitu, *supra* note 6, at 200-01.

13. M.A. Hannan Bin Azhar & Thomas Edward Allen Barton, *Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms*, *in* GLOBAL SECURITY, SAFETY AND SUSTAINABILITY: THE SECURITY CHALLENGES OF THE CONNECTED WORLD 27 (Hamid Jahankhani et al. eds., 2017).

among states to control the unrestricted arena of the information operations.[14]

This Article will include an exploration of the different operations of information warfare. It will also include an explanation of how challenging it has become for international law to regulate information operations. After a brief introduction to the whole Article in the Part I, Part II will include the definition of information warfare and information operations. Part III will highlight some of the major information operations and strategies of information warriors that are being carried out in the current era. Part IV will discuss how significantly the arena of information warfare has revolutionized the concept of warfare in the current era and how substantially the information operations are augmenting the lethality of hybrid warfare. Part V will include an evaluation of the key challenges that are being faced by international law, especially by the international law of armed conflict, in regulating information warfare. Finally, Part VI will include some suggestions for regulating information operations, primarily by bringing the sphere of information warfare under the broad umbrella of international law. Inferences will be drawn at the end of the Article.

II. WHAT IS INFORMATION WARFARE?

Information warfare is a set of contemporary tactics adopted by states as well as nonstate actors to achieve competitive advantage over their adversaries.[15] These tactics can be deployed with or without the use of force.[16] Generally, information warfare causes intangible damage to the adversary by deteriorating its reputation through propaganda, disinformation, or "fake news," which is carried out via the use of mass media, social media, or similar.[17] However, when the software intrusion methods are used

14. *See generally* Johnson, *supra* note 9.

15. GREENBERG ET AL., *supra* note 1, at 1.

16. Markku Jokisipila, *E-Jihad, Cyberterrorism and Freedom of Speech, in* WAR, VIRTUAL WAR AND SOCIETY: THE CHALLENGE TO COMMUNITIES 94 (Andrew R. Wilson & Mark L. Perry eds., 2008).

17. *See* Nitu, *supra* note 6, at 204. *See also* Anna-Marie Jansen van Vuuren et al., *The Susceptibility of the South African Media to Be Used as a Tool for Information Warfare, in*

to cause damage to the strategically or economically important computer data systems of an adversary, then that intangible damage from information warfare can sometimes also produce tangible damage to the adversary.[18] This happens in particular when the military command and control systems of an adversary are attacked with malware or viruses.[19] If such an attack is launched on weaponry systems such as computer control systems of fighter jets or other expensive military tools, then the damage can be tangible and produce heavy financial losses.[20] Human casualties can also result if weapon systems become out of control—e.g., the crashing of jet planes.[21]

The emergence of information warfare operations can be ascribed to advancements in technology, as most of the dangerous information warfare tactics include the use of advanced technological tools. For instance, the spread of malware, viruses, etc. requires modern computer hacking technologies.[22] Thus, technology is used or misused against an adversary with the intention of either causing intangible damage to the adversary or gaining competitive or strategic advantage over it.[23]

A. Definition of Information Warfare

There is no unanimously accepted definition of information warfare so far. Nonetheless, the definitions presented by the US Joint Chiefs of Staff and the US Air Force are, to some extent, famous in the scholarly world.[24] The former regards information warfare as "information operations" and defines it as "the integrated employment of electronic warfare, computer network operations,

---

PROCEEDINGS OF THE 11TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY 127 (Robert Erra ed., 2012).

18. Robbat, *supra* note 7, at 8–13.

19. GREENBERG ET AL., *supra* note 1, at 1–2.

20. Robbat, *supra* note 7, at 8–13.

21. *Id.*

22. DR. YANA KOROBKO & MAHMOUD MUSA, THE SHIFTING GLOBAL BALANCE OF POWER: PERILS OF A WORLD WAR AND PREVENTIVE MEASURES 105 (2014).

23. *See generally* ROGER DEAN THRASHER, INFORMATION WARFARE: IMPLICATIONS FOR FORGING THE TOOLS (1996). *See also* GREENBERG ET AL., *supra* note 1, at 1.

24. See details provided in the text under the footnote 5 in Christopher Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework,* 827 EUR. J. INT'L L. 825-65 (2001).

psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[25] On the other hand, the US Air Force has defined information warfare as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[26]

These definitions suggest that information warfare is a set of techniques that employ information to achieve strategic or competitive advantage over an adversary. Additionally, the above provided definitions also suggest that gaining such competitive advantage also requires ensuring adequate security from the information operations of the adversary.[27] Hence, the strengthening of security systems would play an essential role in the quest to gain advantage over an adversary in the arena of information warfare.

B. Difference Between Information Warfare and Cyberwarfare

Although there are some similarities between information warfare and cyberwarfare, the scopes of the two fields are significantly different. Information warfare is an older phenomenon than cyberwarfare and has been a fundamental part of conventional war throughout the course of history.[28] On the other hand, cyberwarfare is a relatively new phenomenon, because it has emerged only since the invention of the internet and computers, unlike a number of information warfare operations, which existed long before.[29]

---

25. For details, see U.S. DEPARTMENT OF DEFENSE, THE DICTIONARY OF MILITARY TERMS 261 (2009). *See also* MARCO BOSCINI & LEVERHULME TRUST, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 11 (2014).

26. ATHINA KARATZOGIANNI, THE POLITICS OF CYBERCONFLICT 100 (2006).

27. *Id*.

28. David R. Mets, AIRPOWER AND TECHNOLOGY: SMART AND UNMANNED WEAPONS: SMART AND UNMANNED WEAPONS 139 (2008).

29. Ryan White et al., *The Difference Between Cyber and Information Warfare*, CYBER SECURITY & L. POL'Y (Feb. 20, 2018), https://blog.cybersecuritylaw.us/2018/02/20/the-difference-between-cyber-and-information-warfare [https://perma.cc/3CDP-J6AY].

Primarily, in the sphere of information operations, it is information that is used as a weapon against an adversary.[30] In this regard, the US Joint Chiefs of Staff have recognized three distinct elements of the information operations: these include the physical, cognitive, and informational arenas.[31] The list of endeavors that can be carried out in the sphere of information warfare is quite extensive and includes disseminating propaganda, "fake news," or disinformation through media and social media.[32] It also includes spreading malware and viruses and making denial-of-service ("DDoS") attacks on the military command and control systems of an adversary.[33] On the other hand, cyberwarfare only includes reliance on internet and computers as a means of gaining strategic competitive advantage over an adversary.[34] Cyberwarfare relies on DDoS attacks, computer viruses, hacking, and malware attacks on an adversary's strategically important computer systems.[35] Thus, information warfare is a bigger umbrella, including print and electronic media, computers, software, surveillance, and espionage, while the scope of cyberwarfare is limited to the internet and computers.[36] Cyberwarfare is also only one dimension or discipline in the multidimensional field of information warfare; however, owing to the worldwide emergence of technological revolution, cyberwarfare in the broad spectrum of information warfare is crucially important and, therefore, cannot be neglected.[37]

30. Rex Mbuthia, *Cyber Warfare Versus Information Warfare: Two Very Different Concepts*, LINKEDIN (July 16, 2017,) https://www.linkedin.com/pulse/cyber-warfare-versus-information-two-very-different-concepts-mbuthia [https://perma.cc/4QFJ-YZ2W].

31. See ISAAC PORCHE ET AL., REDEFINING INFORMATION WARFARE BOUNDARIES FOR AN ARMY IN A WIRELESS WORLD 12 (2013).

32. *See* GREENBERG ET AL., *supra* note 1, at 1–2.

33. *See id*.

34. *See* STEVE WINTERFELD & JASON ANDRESS, THE BASICS OF CYBER WARFARE: UNDERSTANDING THE FUNDAMENTALS OF CYBER WARFARE IN THEORY AND PRACTICE 16 (2012).

35. *See* White et al., *supra* note 29.

36. *Id.*

37. *Id.*

III. SOME MAJOR TACTICS OF INFORMATION WARFARE

Information warfare is a complicated arena which relies on numerous tactics that are employed against an adversary.[38] It is pertinent to mention here that the tactics of information warfare are also being adopted in waging hybrid warfare.[39] Thus the similarity of the tactics of information warfare and hybrid warfare indicates toward a close mutual relationship that exists between these two arenas of unconventional warfare.[40] The most common of these tactics are elucidated below.

A. Use of Media

According to Aki-Mauri Huhtinen, information warfare always entails certain objectives aimed at an adversary.[41] These objectives primarily include waging propaganda and disinformation against a rival.[42] For this purpose, manipulated information is disseminated against an adversary through certain mediums, among which mainstream media appears the greatest.[43] A certain kind of perception is crafted of the adversary, which is realized through the use of print and electronic media sources.[44]

1. Psychological Warfare

The media is also regarded as a tool of psychological warfare, because the narrative among the people—shaped by the media—fundamentally affects their psychological comprehension of a particular situation.[45] Primarily, it is the media that shapes people's opinions about any incident, activity, or situation. The media can also incite the sentiments of the public by spreading hatred-oriented information among them about a particular

38. *See, e.g.*, Furgacz, *supra* note 3, at 207.
39. *Id*. at 215.
40. *Id*.
41. For details, see Aki-Mauri Huhtinen, *Different Types of Information Warfare*, *in* ELECTRONIC GOVERNMENT: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS 291 (Anttiroiko Ari-Veikko ed., 2008).
42. *See* GREENBERG et al., *supra* note 1, at 1.
43. *See* Vuuren et al., *supra* note 17.
44. *Id.*
45. *See, e.g.*, WAEL ABDELAL, HAMAS AND THE MEDIA: POLITICS AND STRATEGY 145-46 (2016).

activity or situation.[46] For example, the media can incite patriotic sentiments among people by spreading hatred-oriented disinformation about a competitor nation.[47] The masses may start to believe the disinformation, particularly when the majority of the people have no direct access to the correct information about that particular adversary. Such incidents are observed in totalitarian states, where the government has full control over the media and allows the display of only manipulated content and news on TV channels.[48]

2. The Application of the Framing Theory: Relationship Between Media and Foreign Policy

The use of media as a tool of information warfare is also regarded as soft part of information warfare.[49] To explain this further, the "framing theory" becomes applicable.[50] That is, the media frames a particular activity or entity of having certain attributions and promotes its manipulated interpretations of that activity.[51] Such framing can either demonize or glorify that entity depending upon the negative or positive framing of that entity by media, respectively.[52]

Often, the framing theory becomes relevant in shaping the determinants of nations' foreign policy, in which adversary states are regarded as evil and negative, while friendly states are given a positive reputation. This is constructed with or without the use of proper factual information.[53] The foreign policy of the state is shaped by various factors, such as the geopolitics of the state,

46. For example, media can incite patriotic sentiments among the public. For details, see LYN GORMAN & DAVID MCLEAN, MEDIA AND SOCIETY INTO THE 21ST CENTURY: A HISTORICAL INTRODUCTION 82 (2d ed. 2009).

47. *Id.*

48. *See, e.g.*, *id.*

49. For details, see Huhtinen, *supra* note 41, at 292.

50. To understand the framing theory, see Ingrid Volkmer, *Framing Theory*, *in* 1 ENCYCLOPEDIA OF COMMUNICATION THEORY 408 (Stephen W. Littlejohn & Karen A. Foss eds., 2009).

51. Ashli Quesinberry Stokes, *Clinton, Post-Feminism, and Rhetorical Reception on the Campaign Trail*, *in* THE 2008 PRESIDENTIAL CAMPAIGN: A COMMUNICATION PERSPECTIVE 133 (Robert E. Denton, Jr. ed., 2009).

52. *Id.*

53. INGA VON DER STEIN, THE MEDIA AS AN INSTRUMENT OF INFORMATION WARFARE (2016), *available at* https://www.grin.com/document/337247 [https://perma.cc/VN6S-2RSV].

which, of course, are obviously accounted by the media in spreading any narrative about any aspect or issue.[54] However, foreign policy and the media's narratives are significantly influenced by "the political and economic systems of the state."[55] This is evident from the Cold War era, especially during Ronald Reagan's reign in power, when the US media vehemently opposed the socialist and communist agendas of the Soviet Union.[56] In that era, rigorous media campaigns demonizing communist theories were launched by the US mass media.[57] At the same time, US governmental agencies, especially the Central Intelligence Agency ("CIA"), also supported antisocialist narratives.[58] Both the US media and the government's foreign policy were "framing" the Soviet Union and its communist agenda as a threat to the entire world.[59] In fact, the threat did not loom over the entire world but only over the capitalist system prevalent in the United States during the Cold War era, and the democratic political system of the United States could not afford any kind of demise of the capitalist system.[60] Thus, for the strength and dominance of its capitalist system in opposition to the Soviet Union's communism and socialism, the US government relied on its media to launch information warfare against the Soviet's communism. Concomitantly, the US media relied on the information available to it, as interpreted in accordance with US foreign policy regarding the threats posed by socialism and communism to the capitalist economic and democratic political system of the United States.[61] Consequently, the US media launched antisocialist and anticommunist propaganda campaigns against the Soviet Union.[62] Thus, the framing of a particular issue in the foreign policy of a state is reflected in the information disseminated by the media

54. *Id*.

55. *Id.*

56. NANCY BERNHARD, U.S. TELEVISION NEWS AND COLD WAR PROPAGANDA, 1947–1960, 43-45 (2003).

57. *Id.*

58. *Id. See also* GORMAN & MCLEAN, *supra* note 46, at 133,

59. *See* GORMAN & MCLEAN, *supra* note 46, at 133.

60. *See* JAMES R. ARNOLD & ROBERTA WIENER, COLD WAR: THE ESSENTIAL REFERENCE GUIDE, XIII (2012). *See also* SAM AARONOVITCH & RON SMITH, THE POLITICAL ECONOMY OF BRITISH CAPITALISM: A MARXIST ANALYSIS 143 (1981).

61. For example, as described by GORMAN & MCLEAN, *supra* note 46, at 133.

62. *Id.*

about that issue.[63] Furthermore, by relying on such media agencies, it becomes quite convenient for a state to launch information warfare via disinformation and propaganda against its adversary.

B. Reliance on Social Media Platforms

In the contemporary era, owing to the rise of technology and the consequent emergence of smartphones and the use of the internet, social media has appeared as one of the most prominent sources of the dissemination of information.[64] An estimated 3.5 billion people, or nearly half of the human population, use social media.[65] In particular, Facebook has 2.4 billion users, YouTube has 1.9 billion, and WhatsApp, owned by Facebook, has 1.6 billion. These are the most commonly used social media platforms.[66] These forums are the quickest modes of information dissemination as they allow any information to go viral within only a few hours.[67] Furthermore, there are no significant costs associated with the use of almost all of the social media platforms.[68] Social media forums are very convenient and simple to use, and do not require any proper identity verification of the individuals who make the information go viral.[69] Furthermore, the information disseminated through social media platforms keeps on reaching a larger audience. That is, the information can be shared on and on and thus creates a multiplier effect in terms of the number of people it can reach.[70] Therefore, social media is considered a quick way of

63. *See* STEIN, *supra* note 53.

64. Eda Turanci, *Consumption in the Digital Age: A Research on Social Media Influencers*, *in* HANDBOOK OF RESEARCH ON CONSUMPTION, MEDIA, AND POPULAR CULTURE IN THE GLOBAL AGE 269 (Ozlen Ozgen ed., 2019).

65. *See* Simon Kemp, *Digital 2019: Q2 Global Digital Statshot*, DIGITALPORTAL (Apr. 25, 2019), https://datareportal.com/reports/digital-2019-q2-global-digital-statshot [https://perma.cc/3GEG-TXMW].

66. *Id.*

67. *See* Jethro Tan et al., *Building National Resilience in the Digital Era of Violent Extremism: Systems and People*, *in* COMBATING VIOLENT EXTREMISM AND RADICALIZATION IN THE DIGITAL ERA 316 (Majeed Khader et al. eds., 2016).

68. *See* JASON FALLS & ERIK DECKERS, NO BULLSHIT SOCIAL MEDIA: THE ALL-BUSINESS, NO-HYPE GUIDE TO SOCIAL MEDIA MARKETING 233 (2011).

69. *Id.* Read about fake identities on social media as described by R.J. PARKER & J.J. SLATE, SOCIAL MEDIA MONSTERS: INTERNET KILLERS 185 (2014).

70. Automated bot software is also used for this purpose. To read more about bots, see Stefano De Paoli, *A Comparison and a Framework for Investigating Bots in Social*

disseminating information to a large number of audiences.[71] It is regarded as one of the most essential tools of information warfare.[72]

Additionally, another feature is paid campaigns on certain social media websites such as Facebook, which facilitates paid promotion of the content shared on Facebook.[73] This feature makes the shared content visible to a higher number of Facebook users.[74] The price to be paid for such social media campaigns promoting particular content is too small.[75] As campaigns make the content reach a larger audience,[76] they are used by information warriors to wage informational attacks on their adversaries.[77] These informational attacks mainly include the spread of disinformation and propaganda on social media against an adversary.[78] If propaganda or disinformation is spread so as to incite or challenge the religious or ideological inclinations of a nation, then such propaganda can urge them to protest against the individuals sharing propaganda on social media. The resharing of content on social media may further aggravate their emotions and make the information go viral, reaching more people and thus inviting stronger reactions. Such utilization of social media can prove to be detrimental for peace when it is employed by anti-state actors to spread propaganda against the state.[79] Herein, social media appears a negative and lethal component of information warfare as it allows any information to go viral, demonize the

Networks Sites and MMOGs, *in* HANDBOOK ON 3D3C PLATFORMS: APPLICATIONS AND TOOLS FOR THREE DIMENSIONAL SYSTEMS FOR COMMUNITY, CREATION AND COMMERCE 60 (Yesha Sivan ed., 2015).

71. JAY LEVINSON, GUERRILLA SOCIAL MEDIA MARKETING: 100+ WEAPONS TO GROW YOUR ONLINE INFLUENCE, ATTRACT CUSTOMERS, AND DRIVE PROFITS xii (2010).

72. *See* Vuuren et al., *supra* note 17.

73. For details, see KRIS OLIN, FACEBOOK ADVERTISING GUIDE 36 (2009).

74. *Id.*

75. *Id.*

76. *Id.*

77. *See* Vuuren et al., *supra* note 17.

78. TOBY MATTHIESEN, SECTARIAN GULF: BAHRAIN, SAUDI ARABIA, AND THE ARAB SPRING THAT WASN'T 33 (2013).

79. SIMON HARDING, GLOBAL PERSPECTIVES ON YOUTH GANG BEHAVIOR, VIOLENCE, AND WEAPONS USE 117 (2016).

reputation of an adversary within a short passage of time, and incite the emotions of the general public into uproar and tumult.[80]

C. Intrusion of Cyberspace

The intrusion of cyberspace is another tactical move regarded as an element of information warfare.[81] The practice of intruding on cyberspace is dependent on technology. The intrusion of cyberspace is when the strategically important computer systems of an adversary are attacked with viruses or malware via hacking.[82] Many examples of such incidents can be found in recent history and are continuing today. For instance, according to the US Department of Defense, the Pentagon has to foil around 36 million email breaches on a daily basis to secure their computer networking systems from hackers.[83] This highlights the serious nature of the threats posed by technology to the security systems of a state.[84] Therefore, every state tries to maintain strict security over its strategically important data systems.

D. Data Theft

Data theft is also one of the prominent tactics of information warriors.[85] This tactic is motivated by the goal of either thieving confidential and strategically important information from an adversary or stealing funds from the bank accounts of a rival.[86] The consequences may produce intangible damage in terms of stealing strategically important information and may leave the affected party at a strategic disadvantage compared to its rivals.[87] Sometimes, the data theft is politically motivated and is aimed at maneuvering or affecting political situations. A recent example of

80. *Id.*

81. *See* GREENBERG ET AL., *supra* note 1, at 1.

82. *Id.*

83. Frank R. Konkel, *Pentagon Thwarts 36 Million Email Breach Attempts Daily*, NEXTGOV.COM, (Jan. 11, 2018), https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149 [https://perma.cc/63U6-6EPE].

84. *Id.*

85. *See* GREENBERG ET AL., *supra* note 1, at 2.

86. *Id.*

87. *See* GREENBERG ET AL., *supra* note 1, at 2.

such data theft is the Cambridge Analytica scandal, in which the data of as many as 87,000 Facebook users was accessed by one of the board members of the firm Cambridge Analytica.[88] This data was used for the presidential election campaign of Donald Trump in 2016.[89] According to the investigation reports, the data was accessed through an online software application created by an independent researcher and lecturer at Cambridge University, Alexandr Kogan.[90] The name of the application was "This Is Your Digital Life" and it was basically a personality test application.[91] The app became famous among Facebook users and whoever accessed and used the app for a personality test unintentionally gave his/her entire Facebook data and that of his/her Facebook friends to Kogan's app; Kogan later shared this data with Cambridge Analytica.[92] Primarily, the data was of US and UK citizens.[93] This occurred in 2015, when Donald Trump's political team was busy in the election campaign, and one of the members of Trump's political team, Steve Bannon, happened to be a member of the board of Cambridge Analytica.[94] So, he used Kogan's app data for Trump's election campaign and, consequently, Trump's political team crafted the content of Trump's speeches as well as many other election campaigning endeavors and narratives according to the interests and likes of the people whose data was

88. *See* Olivia Solon, *Facebook Says Cambridge Analytica may Have Gained 37m More Users' Data*, GUARDIAN (Apr. 4, 2018), https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought [https://perma.cc/74YR-T8HG].

89. Ian Sherr, *Facebook, Cambridge Analytica and Data Mining: What you Need to Know*, CNET 18 (Apr. 18, 2018), https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/ [https://perma.cc/35CC-N3BY].

90. *Id.*

91. *Id.*

92. See how Facebook users gave their data to Kogan's app as explained in Andrew Wyrich, *What Is Cambridge Analytica, the Data Firm Connected to the Trump Campaign?* R, (Mar. 19, 2018) https://www.dailydot.com/layer8/what-is-cambridge-analytica [https://perma.cc/E4LF-2QKY]. See also how Kogan shared data with Cambridge Analytica as explained by Solon, *supra* note 88.

93. *See* Solon, *supra* note 88.

94. The Editorial Board, *Facebook Leaves Its Users' Privacy Vulnerable*, N.Y. TIMES, (Mar. 19, 2018). https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica-privacy.html [https://perma.cc/8GM6-HYZV].

accessed.[95] Hence, the attempt to affect the US presidential election result was made through the theft of the personal data of thousands of US citizens without their permission.[96]

It was speculated that Russia might have supported the data theft and assisted Trump's political team to access the stolen data via Cambridge Analytica to pave the way for Trump's win in the presidential election.[97] Although the investigations were also made, no conclusive evidence could be traced of the Russian state's involvement.[98] Nonetheless, the mere speculation of such interventions raised alarm bells. The likelihood of such interventions in the future as part of Russia's information warfare strategy could not be neglected.[99] Therefore, it increased calls to regulate social media forums, software applications, and other tools of information warfare to prevent data theft and cyberattacks from making political disruptions in the future.[100] Consequently, the Honest Ads Act became more strictly enforced all over the United States.[101] This law makes it mandatory for all social media and software companies to share their policies and procedures with the US State Department regarding running any kind of application that could access individuals' data and could be used for political purposes.[102] Any application that may appear to have the potential to be used for political purposes, especially any linkages with foreign political powers, might not be allowed to operate in the United States.[103] Thus, through implementing such legal enactments, the US governmental agencies are trying to counter the threats of information warfare that loom over their

95. *See* Sherr, *supra* note 89.

96. *Id.*

97. *Id*. *See* Sherr, *supra* note 89; see *also* Donna Brazile, *Russia's Interference Spotlights Weaknesses in US Election Process*, *in* INTERFERENCE IN ELECTIONS 75 (Kristina Lyn Heitkamp ed., 2018).

98. For details, see the conclusive paragraphs of the article by Sean Illing, *Cambridge Analytica, the Shady Data Firm That Might be a key Trump-Russia Link, Explained*, VOX, (Apr. 4, 2018), https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie [https://perma.cc/D5MA-5PDG].

99. *See id.*

100. *See* Brazile, *supra* note 97.

101. *Id.*

102. *See* Sherr, *supra* note 89.

103. *See* Brazile, *supra* note 97, at 75.

political and security infrastructures.[104] As Cambridge Analytica's cofounder—Christopher Wylie—said himself regarding the threats of information warfare in response to the recent data theft by one of the board members of the firm causing a data-theft scandal, "Rules don't matter for them. For them, this is a war, and it's all fair. They want to fight a culture war in America. Cambridge Analytica was supposed to be the arsenal of weapons to fight that culture war."[105]

E. Rhetoric Building of the Masses of the Adversary State

Information warfare often involves the essential purpose of shaping the narratives of the masses.[106] This is done by spreading manipulated information to them.[107] A state or its agencies can perform this function with or without using the services of media. For example, within the territorial boundaries of a state, the media may be used for this purpose.[108] However, when a state or its agencies aim to construct a particular narrative of the people of its adversary state, they may resort to other covert or overt activities; for instance, they can send their agents into the adversary state, disguising their identities and spreading particular narratives among the general public.[109] On the other hand, some other initiatives—such as establishing nongovernmental organizations ("NGOs") in the adversary state—can also work as tools for waging information operations. Such NGOs may outwardly present their identities as trustworthy organizations working for the development of local people, but, underhandedly, they may be working to spread a particular anti-state narrative among the masses by simply approaching them.[110]

---

104. For example, see how the Pentagon is averting hacking threats as mentioned by Konkel, *supra* note 83.

105. *See* Wyrich, *supra* note 92.

106. ARMIN KRISHNAN, WHY PARAMILITARY OPERATIONS FAIL 237 (2018).

107. *Id*.

108. *See* Abdelal, *supra* note 45. *See also* Huhtinen, *supra* note 41, at 292.

109. *See* GEOFFREY SMITH, ROYALIST AGENTS, CONSPIRATORS AND SPIES: THEIR ROLE IN THE BRITISH CIVIL WARS, 1640–1660 8-9 (2013).

110. For example, some NGOs were banned by the Interior Ministry of Pakistan as they were found to be involved in antistate activities. For details, see Irfan Haider, *Pakistan Will Not Allow NGOs Working* Against *National Interest: Nisar*, DAWN (June 12, 2015), https://www.dawn.com/news/1187773 [https://perma.cc/G7RU-FDDW].

A unique example of using information warfare to build a public narrative of an adversary state was used by the United States in Iraq in 2003.[111] The intention of such information warfare was to pave favorable conditions for its use of force in Iraq, so as to minimize resistance from Iraqi forces and citizens. A few months before the United States attacked Iraq, the United States published manipulated information in pamphlets and flyers and successfully disseminated them to Iraqi citizens and key army officers.[112] The content of some pamphlets urged Iraqi military officers not to destroy the oil wells in Iraq on the orders of the then Iraqi president, Saddam Hussein.[113] The pamphlets presented the narrative that the oil wells were the property of the Iraqi citizens and, therefore, they must not be destroyed.[114] Furthermore, the pamphlets contended that the United States would protect those oil wells if Saddam Hussein gave orders to destroy them in the act of war.[115] This is how the United States tried to deceive the Iraqi people and the international community: by presenting a narrative that the United States was working for the interests of the Iraqi citizens, while the Saddam Hussein's establishment was working for its own interests. The US government presented the same narrative to US Citizens to gain support for the aimed attack in Iraq.[116] Hence, through such dissemination of a manipulated narrative, the United States invaded Iraq and faced no significant resistance in its takeover of the entire Iraqi territory.[117] Ultimately, the US Army got information about the hideout of Saddam Hussein, who was arrested by the US military forces and taken to court, where a trial was held against him that resulted in awarding him a death sentence.[118] Thus, the information warfare launched by the

111. *See e.g.*, Maxie C. Thom, *Information Warfare Arms Control: Risks and Costs*, INSS OCCASIONAL PAPER 45-47 (Mar. 2006), https://pdfs.semanticscholar.org/4d0e/22a368c6afb68a153d6fdb0411f129409c30.pdf?_ga=2.213952983.1307757924.1583038850-969704245.1580936833 [https://perma.cc/MG4Z-EJD7].

112. *Id*.

113. *Id*.

114. *Id*.

115. *Id*.

116. *Id*.

117. *Id*.

118. For details, see PAUL R. BARTROP, A BIOGRAPHICAL ENCYCLOPEDIA OF CONTEMPORARY GENOCIDE: PORTRAITS OF EVIL AND GOOD 136 (2012).

United States months before invading Iraq proved beneficial for the subsequent use of force by the United States in Iraq.[119]

F. Information Warfare by Terrorists

Sometimes, terrorist or nonstate actors also use information warfare to shape a particular narrative among the general public or among the media agencies.[120] For example, the Taliban used information warfare alongside the lawfare strategy against North Atlantic Treaty Organization ("NATO") forces in Afghanistan back in 2007–08.[121] The Taliban used to disguise themselves among the general public in Afghanistan.[122] Hence, when NATO forces launched military operations or air strikes them, many such operations resulted in the killing of innocent civilians residing in the vicinity of the Taliban.[123] Consequently, the Taliban used the lawfare strategy alongside information warfare against NATO forces to present a demonized picture of the NATO attacks.[124] Using lawfare, they invoked international humanitarian law ("IHL") and presented a narrative that the NATO forces violated IHL with their military operations and air strikes, resulting in the deaths of noncombatant civilians.[125] In their information warfare, they reached out to local and international media agencies and shared with them the pictures, videos, and locations of the innocent civilian casualties resulting from the air strikes of the NATO forces.[126] Consequently, the international media agencies, journalists, and human rights activists denounced the NATO air

119. *See* Thom, *supra* note 111, at 46.

120. JANTJE SILOMON, SOFTWARE AS A WEAPON: FACTORS CONTRIBUTING TO THE DEVELOPMENT AND PROLIFERATION 106-23 (2018).

121. Charles J. Dunlap, Jr., Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts 5, (Carr Ctr. for Hum. Rts. Pol'y, Working Paper, 2001).

122. The Encyclopedia of Middle East Wars: The United States in the Persian Gulf, Afghanistan, and Iraq Conflicts, 911 (Spencer C. Tucker ed., 2010).

123. Charles J. Dunlap, Jr., *Lawfare: A Decisive Element of 21st Century Conflicts*, 54 JOINT FORCE QUARTERLY 34, 36 (2009).

124. *Id*.

125. Trevor Michael Alfred Logan, International Law and the Use of Lawfare: An Argument for the U.S. To Adopt a Lawfare Doctrine 8 (MO. ST. U. Graduate Thesis, 2017), *available at* https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4156&context=theses [https://perma.cc/GT2G-RPSM].

126. Dunlap, Jr., *supra* note 121, at 36.

strikes.[127] NATO's official spokesperson responded to this negative portrayal of air strikes as the consequence of a "strategic battle" by the Taliban.[128] Ultimately, the NATO forces started hesitating in rigorously conducting military operations and air-strikes against the Taliban leaders out of the apprehensions of civilian casualties.[129] This hesitation developed primarily due to the negative image of the NATO air-strikes construed in Afghanistan and also due to the fact that the Taliban leaders started residing in the civilian populous regions.[130] Hence, the effectiveness of the NATO military operations in Afghanistan started to decline.[131] Today, as per official claims by the Afghan government, the Taliban controls over forty-five percent of the territory of Afghanistan,[132] though unofficial claims assert that approximately sixty-one percent of the territory is now controlled by the Taliban and the remaining thirty-nine percent is under the control of the Afghan government.[133] Thus, information warfare by the Taliban has deteriorated the effectiveness of the antiterrorist operations of the NATO and US forces in Afghanistan.

In conclusion, information warfare entails the shaping of the narratives of the general public using certain tools and sources, which include mass media agencies including print and electronic media and social media platforms, software applications for hacking or stealing data, and other tools such as malware, viruses, DDoS attacks, etc.[134] Disinformation, propaganda, the dissemination of manipulated information, spreading malware into adversaries' important computer software systems, and stealing confidential and strategically critical datasets are some of the tactics of information warfare pursued by information warriors.[135] It is not only states but also nonstate actors, including

127. RABBI SIMON ALTAF HAKOHEN, WORLD WAR III - SALVATION OF THE JEWS 66 (2018).

128. Dunlap, Jr., *supra* note 121, at 36.

129. *Id*.

130. *Id*.

131. *Id*.

132. *See* Anwer Iqbal, *US Govt Misleading Americans on Afghanistan: Report*, DAWN (Sept. 9, 2018), https://www.dawn.com/news/1431814 [https://perma.cc/PNM4-UHR2].

133. *See* Rod Nordland et al., *How the US Government Misleads the Public on Afghanistan*, N.Y. TIMES, September 8, 2018.

134. *See* GREENBERG ET AL., *supra* note 1, at 1–2.

135. *Id*.

terrorists and NGOs that employ information warfare techniques to either pressure or gain advantage over their adversaries.[136] Unfortunately, information warfare has spread significantly and is also modernizing its facets in the contemporary era, which is posing a challenge to the international legal experts, who ponder ways to regulate such warfare.[137]

IV. INFORMATION WARFARE REVOLUTIONIZING WARFARE IN THE CONTEMPORARY ERA

Due to the novel strategies adopted by the information warfare, the hybrid warfare has become even more effective.[138] This effectiveness is also influenced by the fact that the tactics of information warfare can also be adopted in hybrid warfare.[139] Thus, whenever the information warfare is waged alongside hybrid warfare or alongside the conventional warfare, it boosts the warfare strategy. This Part will elucidate the revolution that information warfare has brought to the arena of war in the modern era.

A. Waging War Without the Conventional Use of Force

The prevalent adoption of the tactics of information warfare by states and nonstate actors has led to a revolution in warfare in the contemporary era.[140] The key feature of this revolution in warfare is that information warfare does not rely on the use of conventional military force and can cause significant intangible damage to an adversary even without the use of force.[141] Such intangible damage may not be imposed on the adversary by the use of force.[142] Furthermore, the intangible damage is not protected by the international law of armed conflict or by IHL.[143] Information

136. *Id*.
137. *See* Johnson, *supra* note 9, at 453.
138. *See* Furgacz, *supra* note 3, at 207.
139. *Id*.
140. *See* GREENBERG ET AL., *supra* note 1, at 4. *See also* ADRIAN R. LEWIS, THE AMERICAN CULTURE OF WAR: A HISTORY OF US MILITARY FORCE FROM WORLD WAR II TO OPERATION ENDURING FREEDOM 387 (2006).
141. *See* GREENBERG ET AL., *supra* note 1, at 4.
142. *Id*.
143. *Id*.

warfare relies on several other methods such as propaganda through media, DDoS attacks, virus attacks, hacking, and defamation through media or social media.[144] None of these information operations require the use of conventional military force.

In particular, when the military command and control system of an adversary state is attacked and damaged through malware or viruses, then such an attack causes significant damage in terms of tarnishing the reputation of the strength of the national defense system of that adversary state, as well as in making the security of that state vulnerable to cyberattacks.[145] Consequently, the adversary state may never engage itself in any armed endeavor with another state unless it has reapplied the security on its military command and control system.[146] In sum, the malware attack on the military command and control systems of an adversary state without the use of actual military force is strong enough to deter any war or armed attack by that adversary state. A repeat attack by information warriors on its security would further imperil its security and defenses from malware attacks and further put it into a position of significant strategic disadvantage compared to its adversaries. Thus, the effectiveness of information warfare shows how substantially and situationally the wager of information operations can defeat its adversary by simply using malware or virus attacks. This further illustrates how substantially information warfare has revolutionized and altered the face of warfare in the modern era.[147]

B. Making the Internet the Battlefield

Information warfare is making the internet or cyberspace the combat zone, replacing conventional battlefields.[148] The information operations executed in the arena of information warfare do not require the presence of physical combat zones or real battlegrounds.[149] For instance, the use of social media and

144. *See* GREENBERG ET AL., *supra* note 1, at 4.
145. *Id*. at 1.
146. *Id.*
147. *See* Lewis, *supra* note 140.
148. GREENBERG ET AL., *supra* note 1, at 1.
149. *Id*. at 2.

electronic media for disseminating propaganda and disinformation against an adversary, the spread of malware into the strategically or economically important computer systems or military command and control systems of an adversary, the intrusion into the cyberspace of the adversary and the theft of strategically important data of the adversary, etc. are some of the examples of such information operations.[150]

C. Augmenting the Effect of use of Force in the Event of an Armed Conflict

Information warfare can also be deployed along with the conventional use of force.[151] In such an event, information warfare would enhance the impacts of the use of force.[152] For example, as mentioned in the previous section, the United States used information warfare in disseminating pamphlets in Iraq months before attacking Iraq in 2003. That proved successful in fulfilling the objectives of the United States to minimize resistance from Iraqi forces and from Iraqi citizens, which helped the US forces to take over the entire Iraqi territory with no significant trouble.[153]

It is pertinent to mention here that information warfare tactics—when waged alongside the conventional use of military force in an armed attack against an adversary—can cause immense damage to the adversary and can give the attacker a significant competitive advantage over the adversary in an armed conflict. For instance, the attacker can introduce malware into jet fighter computer systems, which may cause them to behave abnormally or crash, causing colossal financial losses to the adversary,[154] or putting their air force at a significant competitive disadvantage.[155] Thus, information operations when deployed alongside the use of force can make the latter more potent and impactful in an armed conflict against an adversary.

---

150. *Id*.

151. *See* Thom, *supra* note 111, at 46.

152. Markku Jokisipila, *E-Jihad, Cyberterrorism and Freedom of Speech*, *in* WAR, VIRTUAL WAR AND SOCIETY: THE CHALLENGE TO COMMUNITIES 94 (Andrew R. Wilson & Mark L. Perry eds., 2008).

153. *See* Thom, *supra* note 111, at 46.

154. *See* Robbat, *supra* note 7, at 13.

155. *Id*.

D. Information Warfare as an Element of Hybrid Warfare

Hybrid warfare is a mixture of different overt and covert activities carried out with or without the use of conventional military force.[156] Hybrid warfare also employs kinetic and non-kinetic, asymmetric, and unconventional means of warfare as part of its hybrid strategy.[157] In this regard, hybrid warfare also employs information as a weapon waged by an entity against its adversary.[158] In such a scenario, information as a weapon is waged as propaganda, disinformation, fake news, or defamation.[159] All of these activities are also the tactics of information warfare, creating an overlapping of strategies between hybrid warfare and information warfare.[160] As hybrid warfare is a broader spectrum of strategies involving the tactics of information warfare, it can be asserted that information warfare is an element of hybrid warfare.[161] Concomitantly, several states as well as nonstate actors are using information warfare in their endeavors of hybrid warfare against their adversaries.[162]

Information warfare tactics, when employed in hybrid warfare, make hybrid warfare more lethal and severe.[163] For instance, when certain activities such as propaganda is waged through news or social media against an adversary, then it can have the tendency to malice the reputation of the adversary.[164] In particular, when propaganda is spread out in a way that it creates a convincing air among the viewers against the adversary, then the

156. Ambassador Sorin Dumitru Ducaru, *Framing NATO's Approach to Hybrid Warfare*, *in* COUNTERING HYBRID THREATS: LESSONS LEARNED FROM UKRAINE 4 (Niculae Iancu et al. eds., 2016).

157. *See* Andrés B. Muñoz Mosquera & Sascha Dov Bachmann, *Understanding Lawfare in a Hybrid Warfare Context*, 37 NATO LEGAL GAZETTE 22 (2016).

158. *See* Furgacz, *supra* note 3.

159. *Id. See also* Barna, *supra* note 4.

160. *See* Barna, *supra* note 4.

161. *Id. See also* Furgacz, *supra* note 3.

162. *See* Barna, *supra* note 4.

163. For example, see how the Russia made its hybrid war in Ukraine more stringent and effective in Ukraine because Russia captured the entire Crimean region, as described in: Sascha Dov Bachmann & Andres B. Munoz Mosquera, *Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach*, *in* A CIVIL-MILITARY RESPONSE TO HYBRID THREATS 67 (Eugenio Cusumano & Marian Corbe eds., 2017).

164. *Id*.

reputation of the adversary becomes tarnished causing it to lose support from the international community.[165]

On the other hand, when other information warfare tactics such as DDoS attacks and hacking are employed in an armed conflict, then the adversary is put into a position of competitive disadvantage in the conflict.[166] For instance, if the command and control system of an adversary is attacked through DDoS attacks or hacking and is controlled against the adversary, then the adversary may face significant damage.[167] This will also put the adversary into a losing position in an armed conflict. Similarly, when the adversary is unable to defend its strategic computer systems from the DDOS attacks, then such an attack damages the reputation of the strength of the defense system of the adversary.[168] The damage to the repute puts the adversary into a position of competitive and strategic disadvantage against its rivals.[169] Thus, the information operations of DDoS attacks will become an element of hybrid warfare due to the covert nature of the operation. The situation will then highlight that a DDoS attack may have installed the hybrid warfare against the affected party through employing information operations.

In sum, information warfare has revolutionized the facets of conventional warfare.[170] It has taken the warfare out of the conventional battlefield and into the arena of the internet.[171] Cyberspace has become the new battlespace, where information warriors can, without shedding opposing soldiers' blood, cause significant intangible damage to an adversary by destroying its reputation, by stealing its strategically important data, or by making its security systems vulnerable to attacks.[172] Furthermore, information warfare has given support to the overt and covert

165. *Id. See also* Furgacz, *supra* note 3.
166. *See* GREENBERG ET AL., *supra* note 1, at 1–2.
167. *Id.* at 2.
168. *Id*.
169. *See* GREENBERG ET AL., *supra* note 1, at 1–2.
170. *See* Lewis, *supra* note 140.
171. *See* GREENBERG ET AL., *supra* note 1, at 1.
172. *Id.*

operability of hybrid warfare.[173] Notably, information warfare has also enhanced the lethality of hybrid warfare in the contemporary era.[174] States and nonstate actors now wage hybrid warfare by only relying upon information warfare tactics and using information as a weapon against their adversaries.[175] Hence, information warfare has made hybrid warfare as easier.[176]

V. INTERNATIONAL LAW AND INFORMATION WARFARE

This Part of the Article includes an explanation of the relevant rules of international law that can be applied to the sphere of information warfare. Some of these rules—for instance the Outer Space Treaty 1967—end up indirectly facilitating the conditions that support the continuation of information warfare, leaving information warfare unchecked under international law. On the other hand, the complex and variegated arena of information warfare makes it challenging for international norms and principles to regulate and control information operations.[177] For instance, although the law of war, the law of armed conflict, and IHL make attempts to regulate the conduct of actors involved in information warfare, the intangibility of the damage caused by information warfare makes it difficult for IHL to impose restrictions on information warfare.[178]

A. The Law of War

The law of war or the law of armed conflict protects civilians and noncombatants in an armed conflict.[179] Likewise, the law of war also attempts to protect civilians from any information warfare attack. That is, the parties engaged in information warfare

173. For example, see how the disinformation campaign by Russia helped it to achieve its objective in its hybrid warfare endeavor in Ukraine, as described in Bachmann & Mosquera, *supra* note 163, at 67.

174. *See, e.g.*, *id*.

175. *See* Furgacz, *supra* note 3. *See also* Barna, *supra* note 4.

176. For example, see how the Russia achieved its objective in Crimea, as described in Bachmann & Mosquera, *supra* note 163, at 67.

177. *See* Robbat, *supra* note 7, at 8. *See also* GREENBERG ET AL., *supra* note 1, at iii.

178. GREENBERG ET AL., *supra* note 1, at 4.

179. *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 29 (2004).

must cause no harm to the civilian population.[180] This rule can be applied to the activity of hacking or the disruption of any technological transmission of an adversary state by a wager of information warfare.[181] If such an activity harms civilians in any manner—for instance in disrupting their businesses, daily routines, etc.—then such an activity ought to be considered illegal under IHL or the law of war.[182] Several other inferences can similarly be made that could ensure protection for civilians and noncombatants.[183]

B. Challenges Faced by International Law in Regulating Information Warfare

In fact, there are many challenges faced by international law, in particular by IHL or the law of war, in regulating information warfare.[184] These challenges mainly derive from the intangibility of the damage brought up by information warfare. Unfortunately, because of such challenges, international law becomes paralyzed in an attempt to regulate or control the broad and complicated field of information warfare.[185]

1. Intangibility

The essential challenge to international law posed by information warfare is the intangibility of the damage caused by the information operations instituted by an entity against its adversary.[186] International law, in particular the international law of armed conflict, is silent on any intangible damage caused to an adversary in times of war and peace.[187] Therefore, it becomes difficult for international law to regulate or restrict those information operations that specifically produce intangible damages in times of war and peace.[188]

180. GREENBERG ET AL., *supra* note 1, at 10–11.
181. *Id.* at 11.
182. GREENBERG ET AL., *supra* note 1, at 12.
183. *Id.*
184. Robbat, *supra* note 7, at 8.
185. *See* Johnson, *supra* note 9, at 453.
186. GREENBERG ET AL., *supra* note 1, at 4.
187. *Id.*
188. *Id.*

a. Unregulated Intangible Damage

What exactly is included under the term "intangible damage" varies according to the mode of information operation launched against an adversary; for instance, when the media is used to wage propaganda against an adversary or when social media is relied on for defaming an adversary, the intangibility resides in damaging the reputation of the adversary.[189] On the other hand, when disinformation is used as a weapon of information warfare, it is intangible in terms of depriving the people of the true information and facts about a certain aspect or activity in times of war or peace. In all of these instances, the damage is not physical or tangible, which ultimately excludes the principles of international law as inapplicable to such situations.[190] Consequently, it becomes impossible to regulate such activities of information warfare pursued by an entity against its adversary.[191]

b. Intangibility Leading to Tangible Damage

There are certain exceptions in which the intangible damage sometimes leads to tangible damage as well. For instance, when the cyberspace of the adversary is intruded via introducing malware or a virus to the strategically important software systems of an adversary, the intangible damage can produce some tangible loss in terms of damage of infrastructure or loss of human lives.[192] For example, hacking the jet fighters of an adversary or attacking them with malware can cause colossal financial loss as well as human casualties.[193] However, international law does not provide sufficient guidance on such conduct of states in times of war and fails to restrict such activities unless they result in harming noncombatants.[194] Thus, in reality, there exist significant gaps in international law in regulating the activities of information warfare.[195]

189. GREENBERG ET AL., *supra* note 1, at 4-5.
190. *Id*. at 4.
191. *See* Johnson, *supra* note 9, at 453.
192. *See* Robbat, *supra* note 7, at 13.
193. *Id*.
194. *Id*.
195. *Id*. *See also* Johnson, *supra* note 9, at 453.

2. The Inherent Right to Freedom of Opinion and Expression

When information warriors use the media or social media to wage propaganda or spread disinformation among the public, then the individual's right to freedom of opinion and expression becomes relevant in providing the freedom to information warriors in using the media or social media to spread the narratives they prefer against their adversary.[196] The right to freedom of opinion and expression is protected under the Universal Declaration of Human Rights, passed by the United Nations in 1948.[197] The text of Article 19 of the Universal Declaration of Human Rights affirms the right in the following words: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[198] In particular, Article 19 permits no interference in the freedom of expression of an individual.[199] The part of the text stating "freedom to hold opinions without interference," thus, makes it challenging for international law to restrict any opinion or expression that is expressed within the spirit of Article 19 of the Universal Declaration of Human Rights.[200]

As the Universal Declaration of Human Rights is an essential element of customary international law, it is therefore customary international law that promotes the right to freedom of opinion and expression.[201] This assertion further restricts international law in regulating or controlling any activity of information warriors carried out in pursuance of their right to freedom of opinion and expression. The only thing that can prevent them from exploiting their right to freedom of opinion and expression for information warfare is the adversary legally proving their

196. *See, e.g.*, NANCY SNOW, THE ARROGANCE OF AMERICAN POWER: WHAT U.S. LEADERS ARE DOING WRONG AND WHY IT'S OUR DUTY TO DISSENT 3 (2007).

197. *See* TIM CROOK, COMPARATIVE MEDIA LAW AND ETHICS 33 (2009).

198. *See* Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) [hereinafter UDHR].

199. *Id*.

200. *Id*.

201. *See* OLIVIER DE SCHUTTER, INTERNATIONAL HUMAN RIGHTS LAW: CASES, MATERIALS, COMMENTARY 50 (2010). *See also* MARTIN DIXON, CASES & MATERIALS ON INTERNATIONAL LAW 209 (2016).

expression of opinion to be defamatory by filing lawsuits against them in a court following the international legal protocols.[202] Through this, information warriors can be legally restricted in expressing their opinions if such opinions are proved legally in court to be hate crime or utterly defamatory.[203] Otherwise, the inherent right to freedom of opinion and expression is exploited or misused by information warriors as a weapon. Hence, the relationship between the tactics of information warfare and the right to freedom of opinion and expression under Article 19 of the UDHR becomes challenging for international law, preventing it from regulating and controlling information warfare. This leads to a perpetual continuation of information operations by states and nonstate actors against their adversaries.

3. The Outer Space Treaty and the CHM Principle

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space Including the Moon and Other Celestial Bodies, commonly known as the Outer Space Treaty, was formally ratified in October 1967.[204] According to this treaty, space and all celestial objects are the common heritage of the whole of mankind.[205] A similar principle has been presented by the Moon Treaty, which was approved in 1979.[206] According to the Moon Treaty, the moon and all its resources are the common property of the whole of mankind.[207] Therefore, from these two treaties, it can be asserted that space and the resources of its celestial objects including the moon are free to use.[208] This assertion was given under the CHM principle, which states that any object or property that is common to the whole of mankind must

202. For instance, see some examples and discussion about defamation cases as described in DAVID STRECKFUSS, TRUTH ON TRIAL IN THAILAND: DEFAMATION, TREASON, AND LÈSE-MAJESTÉ 1 (2010).

203. *See id*. at 414.

204. Stephan Hobe, *Technological Development as a Challenge for the Development of Air and Space Law*, *in* A NEW INTERNATIONAL LEGAL ORDER 296 (Chia-Jui Cheng ed., 2016). *See also* FRANCIS LYALL & PAUL B. LARSEN, SPACE LAW 53 (2016).

205. *See also* PRUE TAYLOR, AN ECOLOGICAL APPROACH TO INTERNATIONAL LAW: RESPONDING TO THE CHALLENGES OF CLIMATE CHANGE 259 (2008).

206. *Id*.

207. *Id*.

208. *Id*.

be free to be used by all nations.[209] The CHM principle alongside the Outer Space Treaty is applicable to information warfare, because most information operations are carried out through the transmission of radio waves, which travel through space.[210] That is, whether it is the telecasting of news from a radio or television channel, the spreading of information through social media platforms, or the intrusion of cyberspace through hacking via the internet, radio waves are employed, transmitted from artificial satellites sent to space by the major international telecommunication agencies or by some governments.[211] Hence, whenever any of the aforementioned activities of information warfare take place, space becomes the medium of transmission of radio waves and, hence, facilitates the pathways of information operations. Concomitantly, as, in accordance with the Outer Space Treaty and the CHM principle, space is the common property of the entire mankind and is free to use for all humanity, the utilization of space is therefore free for everyone, even for carrying out information warfare operations.[212] Hence, indirectly, the Outer Space Treaty and the CHM principle provide legal protection for the continuation of information warfare operations.

Thus, international law has stringent limitations in regulating the sphere of information warfare.[213] The limitations are mainly attributed to the intangibility of the damage caused by information warfare.[214] The intangibility is not addressed in the international law of armed conflict; therefore, how to regulate the arena of information warfare becomes uncertain.[215] Furthermore, international protection of the inherent right to freedom of opinion and expression—as constituted in Article 19 of the UDHR—further consolidates the inability in international law to regulate certain

209. GILLIAN DOREEN TRIGGS & JOHN ROBERT VICTOR PRESCOTT, INTERNATIONAL FRONTIERS AND BOUNDARIES: LAW, POLITICS AND GEOGRAPHY 402 (2008).

210. For instance, as described by Medoff and Kaye that every media company relies on satellite telecommunication for transmission of information. Satellite communication employs radio waves. For details, see NORMAN J. MEDOFF & BARBARA KAYE, ELECTRONIC MEDIA: THEN, NOW, AND LATER 9 (2016).

211. *See id. See also* DIANE POREMSKY & SHERRY KINKOPH GUNTER, OUTLOOK 2013 ABSOLUTE BEGINNER'S GUIDE 46 (2013).

212. *See* TAYLOR, *supra* note 205.

213. *See* Johnson, *supra* note 9, at 453.

214. GREENBERG ET AL., *supra* note 1, at 4.

215. *Id*.

information operations such as the waging of propaganda against an adversary through media or social media.[216] Additionally, the Outer Space Treaty and the CHM principle allow the dissemination of information through the radio waves transmitted from the artificial satellites sent into space, even if such information is deployed or used by information warriors in their respective information operations.[217] Thus, indirectly, or inadvertently, international law appears to facilitate information operations instead of regulating or controlling them. Therefore, it has become problematic for international legal experts to devise ways to control information operations.[218]

VI. SUGGESTIONS TO REGULATE INFORMATION WARFARE

The legal challenges in regulating information warfare need to be addressed and evaluated by the international community to control the threatening rise of information operations by states and nonstate actors waging information warfare or hybrid warfare against their adversaries. This Part of the Article includes some suggestions for paving the way to regulating information warfare to bring it under the legal authority of international law. One suggestion is to enact new laws, rules, and principles as well as to draft a new convention to not only regulate information warfare but also eliminate the challenges caused by the other treaties and principles of international law in controlling the arena of information warfare.[219]

A. Enact New Laws, Rules, and Principles

At present, there is no particular set of rules or policies under the wide umbrella of international law that could define or regulate information operations.[220] The legal vacuum is massive in this regard, and it needs to be closed to discourage the harmful employment of information warfare.[221] This vacuum can be filled

216. *See* UDHR, *supra* note 198, art. 19.
217. *See* MEDOFF & KAYE, *supra* note 210. *See also* TAYLOR, *supra* note 205.
218. GREENBERG ET AL., *supra* note 1, at 4.
219. *See* Johnson, *supra* note 9, at 439.
220. *Id.*
221. *See* Johnson, *supra* note 9, at 453.

if new rules or principles are devised under the umbrella of international law to regulate the conduct of parties engaged in information warfare.[222] For this purpose, the existing laws and principles pertaining to curbing hate speech can be made the foundations for enacting the new laws.[223] A pertinent collaboration of the international community might prove helpful in this regard as certain states, e.g., European and Scandinavian states, may share their successful experiences in curbing hate speech, disinformation, and propaganda in their domestic arenas.[224] Here, states should also collaborate with one another to discuss various aspects, tools, and areas on which special legal controls are required for regulating the complicated arena of information warfare.[225] For instance, the use of the media to disseminate false information is an active platform for the wagers of information warfare against their adversaries.[226] Therefore, this platform has to be analyzed and then carefully regulated in a manner that not only protects the necessary freedom of opinion and expression, but also controls any kind of negative activity pursued through the media within the sphere of information warfare. It is suggested that a special code of conduct has to be formulated at the international level, drafted particularly for the international news media agencies, to prevent or criminalize the propagation of

222. *Id*. at 439.

223. For example, as described in this book about the defamation laws controlling hate speech: STRECKFUSS, *supra* note 202, at 1 (see also pages 103 and 414 of the same book. Such laws can be enacted and made prominent at the international level for regulating the hate speech, defamation, and disinformation activities of information warriors).

224. Western European nations and Scandinavian states have been regarded as having adopted the laws curbing hate speeches alongside protecting the freedom of opinion and expression. The legislators of these nations should be consulted about new rules and principles for regulating the activities of information war. For details about EU hate speech laws, see Sejal Parmer, The Legal Framework for Addressing "Hate Speech" in Europe, at 3, *presented in* Addressing Hate Speech in the Media: The Role of Regulatory Authorities and the Judiciary, in the International Conference Organized by Council of Europe in Partnership with the Croatian Agency for Electronic Media (Nov. 6–7, 2018).

225. For instance, see a recent special regulation in Europe for curbing hate speech: William New, *New EU Directive Limits Hate Speech, Establishes European Content Quotas*, INTELL. PROP. WATCH (Nov. 6, 2018,) https://www.ip-watch.org/2018/11/06/new-eu-directive-limits-hate-speech-establishes-european-content-quotas [https://perma.cc/DF5D-7QDB].

226. For example, as described by Vuuren et al., *supra* note 17, at 127.

propaganda and hate speech.[227] The new regulations should include the curbing of negative propaganda against states, religions, races, ethnic communities, etc. Whether such a policy is implemented assertively or normatively is another question to be dealt with and one that the international community has to decide after evaluating the advantages and disadvantages of each strategy. Nonetheless, the rules and principles aiming at curbing fake news, hate speech, and propaganda may be implemented in a normative sense, but their normativity may make them assertive in the future if the entire international community or even the United Nations ends up positively endorsing them. Thus, in the same way, all other aspects of information warfare can be dealt with and regulated.

B. Arrange a New Convention: The Need of the Hour

At present, there is no single convention on the issue of regulating information warfare.[228] On the other hand, states and nonstate actors have started actively relying on the use of information warfare tactics against their rivals,[229] which poses a serious threat to international peace and security. In particular when terrorists wage information—as the Taliban benefitted from resorting to information warfare alongside their lawfare strategy against the NATO forces in Afghanistan,[230]— it consequently undermines the effectiveness of operations against them. As previously stated, the Taliban now have control of nearly half of the territory of Afghanistan.[231] Thus, because of such threats, international legal experts have raised their voices and scholars endorse the arrangement of a new international policy or convention to regulate the growing phenomenon of information warfare in the contemporary era.[232] Though these calls have not

227. For example, as such a policy has been recently implemented in Europe. For details, *see* New, *supra* note 225.

228. *See* Johnson, *supra* note 9, at 453.

229. Cristian Barna, *The Road to Jihad in Syria: Using SOCMINT to Counter the Radicalization of Muslin Youth in Romania*, *in* COUNTERING RADICALIZATION AND VIOLENT EXTREMISM AMONG YOUTH TO PREVENT TERRORISM 193 (Marco Lombardi et al. eds., 2015).

230. Dunlap, Jr., *supra* note 121, at 36.

231. Nordland et al., *supra* note 133.

232. *See* Johnson, *supra* note 9, at 439.

gained momentum so far, the rationality and practicality behind them are quite convincing, and the world needs to consider this earnestly.[233]

If the calls for a new convention on regulating information warfare are heard positively and a new convention is arranged, then the convention would provide a new and rigorous forum for analyzing and regulating the different arenas of information warfare. In particular, it would provide a special forum for states, legal experts, and the bodies of international law to discuss the various aspects of information warfare and listen to one another's suggestions for regulating it. Consequently, they could unanimously devise a new code of conduct or rules to regulate information operations.[234] Additionally, it would also close the existing loopholes in international law, which are indirectly facilitating information warfare—for instance the Outer Space Treaty[235]. Hence, it is the need of the hour to arrange a new convention to bring information warfare under the authority of international legal norms, rules, or principles, as doing so will help mitigate the threats posed by information operations to international peace and security.[236]

VII. CONCLUSION

In the contemporary era of technological advancement, information warfare is being deployed by states and nonstate actors against their adversaries.[237] Information warfare entails the dissemination of manipulated information or the access to particular information and then using that information to acquire competitive advantage over an adversary.[238] Some examples of information warfare include the spreading of propaganda or disinformation through the use of mass media, the spread of malware or viruses into computerized military command and control systems or other strategically important institutions, the theft of important data via hacking, and the demonization of the

233. *Id*. at 453.
234. *See* Johnson, *supra* note 9, at 439.
235. *Id*.
236. *Id*.
237. *See* Barna, *supra* note 4.
238. *Id*. *See also* Nitu, *supra* note 6.

reputation of an adversary via the use of electronic media or social media platforms.[239]

All of these tactics of information warfare are revolutionizing the face of warfare in the current era.[240] The war is now being waged on new fronts, particularly on technological fronts, because states and institutions have recognized the importance of strengthening the security systems of their strategically important datasets and computer systems.[241] The threat from hackers is prevalent and massive; they can cause a significant amount of damage, ranging from destroying a reputation to causing huge financial losses and theft of confidential data reports.[242] For this purpose, state institutions are deploying special security measures to avert the threats of information warfare.[243]

Certain tactics of information warfare can prove to be deadly for international peace and security; for instance, disinformation and propaganda are tactics that can aggravate tensions among adversary states, leading to conflict if the states get engaged in perpetual propaganda wars against each other.[244] Furthermore, the tactics of information warfare when deployed by terrorist organizations can also cause detrimental damage to regional or international peace.[245] The situation may be very critical if the terrorists get their hands on the hacking strategy and can spread malware or viruses or take control remotely over the strategically important computer systems of an adversary state.[246] In such an event, the threat to regional peace and damage to the reputation of the security of the state could be massive. Therefore, it is the need of the hour to regulate the tactics of information warfare before it gets too late to do so.

Nonetheless, despite the aforementioned threats to international peace and security, there has unfortunately been no mechanism, policy, or set of rules devised at the international level

239. *See* Nitu, *supra* note 6. *See also* GREENBERG ET AL., *supra* note 1, at 2.

240. *See* LEWIS, *supra* note 140.

241. *See* GREENBERG ET AL., *supra* note 1, at 1.

242. *See, e.g.*, Greenberg et al., *supra* note 1, at 2.

243. For example, see how the Pentagon is averting hacking threats in Konkel, *supra* note 83.

244. *See* Konkel, *supra* note 83.

245. *See id*.

246. *See id.*

that could regulate the arena of information warfare.[247] Moreover, there is not even a single convention under the wide umbrella of international law so far that has discussed the need to regulate or control information warfare.[248] Although there have been calls raised by a number of legal experts to draft a new convention under the authority of international law to regulate the arena of information warfare, such calls have not gained momentum so far.[249] A trend seen over the past few decades has been that the international community does not take into consideration calls for drafting a separate convention on any issue unless that particular issue becomes global and very significant in nature.[250] Thus, no special efforts have yet been made to draft either a separate convention or special rules that could hear the calls to regulate information warfare.[251] It can only be hoped that—if not at present, then in the future—the calls to regulate information warfare will gain momentum.

247. *See* Johnson, *supra* note 9, at 453.
248. *Id*. at 439.
249. *Id*.
250. *Id*.
251. *Id*. at 453.