HYBRID WARFARE – CHALLENGES FOR PAKISTAN

Dr. Tughral Yamin[*]

Abstract

In order to achieve political aims; the traditional means of kinetic warfare have always been supplemented by aggressive diplomacy, economic coercion, intelligence gathering, propaganda and proxy wars. A combination of all these tools is essential for a nation to achieve its political goals set out to win a war. All through the ages, technology has played a significant role in enhancing the capacity and capability of nations to win wars. The tools of modern warfare based on cyber and information technology has transformed the nature of warfare. Social media in particular is being used subtly as well as aggressively to shape public opinion and weaken the morale of the nation. The geographical dimensions of the battlefield have been eliminated. War is now waged in the minds of not only the opposing commanders but also in the minds of the nation. The dictum that strategy is the dialectic of opposing will is truer now than ever before. Wars can now be won without firing a single bullet. This changed nature of warfare needs to be understood in its entirety. While contingency plans exist in military headquarters to counter a physical invasion, there is little by way of collectively responding to the threats launched from various technical platforms. This paper is an attempt to look into the transformation of war fighting and suggests a few policy options for Pakistan to take up the challenges of hybrid warfare and keep the national will and morale intact during the worst of times.

Keywords: Cyber Warfare, Social Media, Propaganda, National Will, Morale and Public Opinion.

Introduction

As per famous military sage Karl von Clausewitz, war is the extension of policy by other means. In order to fulfill a policy objective, kinetic means of warfare have always been supplemented by diplomatic pressure and economic coercion; intelligence gathering and propaganda; espionage and proxy wars. A balanced combination of all these means and other traits and characteristics such as the quality of leadership and the resilience of a nation in adversity; and the economic

[*]The author is the Associate Dean at the Centre for International Peace & Stability (CIPS), National University of Sciences & Technology (NUST) Islamabad and Aizah Azam who is a MS in Peace & Conflict Studies from Centre for International Peace & Stability (CIPS), National University of Sciences & Technology (NUST) Islamabad helped the author during the development of this article. The authors' email address is adeancips@nipcons.nust.edu.pk.

and political standing of a nation and internal stability are instrumental in leading to the successful culmination of the war effort.

Ever since the Stone Age, technology and scientific innovation have played an important role in ushering in successive waves of revolution in military affairs. These scientific discoveries have increased the power potential of nations manifold through the introduction of such revolutionary means of conducting warfare such as gun powder; wind, steam and fossil fuel energy to propel battleships and battle tanks; and nuclear power to cause widespread death and destruction. Technology is now moving at a phenomenal speed to bring about fundamental changes in the nature of warfare. The theatre of warfare has drastically expanded from its pre-established definitions due to the introduction of 'virtual' battle spaces. The discourse on warfare is now more technologically driven than before. It has become elusive in character and is marked by the creation of abstract settings and use of multiple means of power to establish supremacy and achieve the political goals. This has led to the elimination of physical barriers and has empowered hidden forces that can manoeuvre and defeat the adversary without fighting an actual battle. It has become a mind game and Andre Beufre's famous dictum that strategy is the dialectic of opposing wills, has now become the absolute truth.

Scholars and academics refer to this transition as the 'hybridization' of warfare. In all honesty, there is little agreement on what actually constitutes a hybrid threat and what does not but there is substantial agreement over its existence and the fact that states use hybrid tactics in modern times for the extension of their political and economic goals. The term 'hybrid warfare' was used for the first time by Frank Hoffman. Hoffman asserted that hybrid threats fundamentally comprised simultaneous usage of conventional competencies coupled with other asymmetrical tactics, which portray a stride of criminality. Hoffman, like others before him and like those who followed him did not identify the actors engaged in the use of hybrid tactics and / or the targets. The basic explanation of the synchronized deployment of forces, both regular and irregular is rooted in producing a well-coordinated synergistic effect encompassing both, the physical and psychological dimension of conflict. These effects, he believed could be gained at all levels of warfare i.e. tactical, operational as well as strategic. Hoffman's understanding of hybrid wars described the conduct and use of force as the conjunction of regular and irregular threats through the use of sophisticated technology and decentralized system of execution. He built this idea by positing hybrid warfare as the synergistic fusion of conventional and unconventional forces in conjunction with terrorism and criminal behaviour. This fusion was oriented towards a desired objective through a political narrative, which simultaneously and adaptively unified all the elements of the force.[1]

Hybrid wars can hence be defined as coordinated and often simultaneous deployment of multiple instruments of power and influence aimed at exploiting the adversary at every level from leaders to citizens. Most vulnerable in fact is the latter so tactics deployed constitute non-linear, ambiguous and yet a cognitive manipulation of the adversary population.[2] Of the many intriguing features of hybrid warfare, one of the most perplexing is the inherent ambiguity in its conduct. There is definitely a definitional dilemma in this form of warfare, when it comes to the delineation of Actors i.e. who wages it? Tactics i.e. what means are deployed for it? Timeframe of the engagement i.e. how long would the hostilities stretch? and most importantly the Repercussions i.e. what are its effects? It is this ambiguity in the character of hybrid warfare that adds to the challenge of defining it and eventually deterring and preventing it. The hybridization of warfare has blurred the demarcations/distinctions between the physical and virtual domain; combatants and non-combatants; and state and non-state actors. It has added to the complexity of effectively defining risk and threat to state security by broadening the basis of the perils and pitfalls in this kind of nebulous warfare.[3]

With a broadened risk base, hybrid tools to conduct war beyond the concrete battle spaces have come to include cyber-attacks on national databases, hostile narrative building through propaganda, misinformation and disinformation through social media. The main objective is to hurt the adversary at the psychological and cognitive level, without necessarily causing any harm within the physical space.[4] There are limited restrictions when it comes to the use of available resources. In this connection, hybrid wars have often times been referred to as 'unrestricted warfare' as well. This unrestricted arena of warfare works with completely transformed notions of weaponry such as resorting to the use of computer viruses during combat operations. However, it must be noted that the core aim of the use of these reformed techniques, remain purely Clausewitzian, that is to cloud the adversary's judgment and decision making, compelling it to surrender to one's own planned agendas, without using any overt force.[5]

Considering factors such as unhindered access to virtual spaces and their manipulation by state parties and shadowy non-state actors all dabble in hybrid war to achieve their political ends. Often times they operate silently by remaining under the radar to escape notice till it is too late. Axiomatically, therefore, the impact of hybrid means of warfare cast on the nation now constitutes a critical aspect of national security paradigms. Needless to say, the national will can be broken if the enemy is allowed to operate with impunity. Clearly, the planners and decision makers of modern wars must be able to comprehend, shape and reinforce national behaviours and opinions. This is only possible by creating legitimately good 'information'.[6] Doctored or malicious 'information' based on propaganda and fake news can cause terrible harm to the morale of the nation. In the recent times, some significant changes in a nation's inherent will to resist have fallen victim to the coordinated propagation of fake news and malicious untruths to influence public opinion.

Pakistan is confronted by a wide array of multi-dimensional threats. Hostile forces are in full play to isolate it internationally. Terms like 'irresponsible' state and 'sponsor of state terrorism' are used liberally to malign it. Money and agents provocateurs are being used to weaken the national resolve. The aim is to create an image of a weak and vacillating national leadership that lacks the ability to comprehend or manage the developing situation. The strands of hybrid threats are built upon 'credible' psy ops themes through an offensive propaganda spread by traditional means such as print and electronic media and not traditional means such as social media campaigns; threat of cyber-attacks; looming risk of economic coercion to the risk of political isolation on the global stage.[7]

Unfortunately, despite evident risks, the national thought process to respond to hybrid threats remains archaic and outdated. There is only a limited understanding of the security threats and there is a lack of imaginative responses to this nebulous threat. The planning and execution of Pakistan's security policies with reference to India are built up around frameworks such as the Cold Start Doctrine (CSD) or the Proactive Strategy (PAS).[8] The response is more in military terms and the redlines are in geographical terms. The defensive strategies have been recycled from previous wars and war like experiences. There is a need for a fresh approach to respond to the hydra headed monster of hybrid warfare.

The well-defined military offensive across the international border within the overarching framework of CSD and PAS is being replaced. The Indian civil and military leadership has changed tack and is now talking about launching surgical strikes across the Line of Control (LoC). The Indian army chief Gen Bipin Rawat has claimed that his forces had carried out such strikes in 2016 in response to Pakistani backed strikes by Kashmiri freedom fighters against border outposts in places like Uri in Occupied Kashmir and Pathankot. A new movie titled *Uri: The Surgical Strike* set for release early this year emphasizes the capability of conducting such fanciful strikes into Azad Kashmir.[9] It is naturally blatant propaganda aimed to raise their own morale and to depict the Pakistani forces in poor light.

Noted academician and current federal minister for human rights Dr Shireen Mazari is of the opinion that the purpose of the Indian hybrid warfare is to strike at the Centre of Gravity (CoG) of Pakistan.[10] The CoG is the fighting spirit of the general public. If they know that their national leadership is strong and their armed forces capable of repelling and deterring all kinds of attacks, whether these are physical, political or financial, they can survive all the propaganda and fake news being spewed out to weaken their resolve. Propaganda and intelligence gathering it may be noted were recommended tools of war enshrined in Arthashastra - ancient Indian Hindu strategist Kautliya's famous treatise on statecraft.

Social Media

In this age of hybrid warfare, it is instructive to study how social media influences the minds of the citizens of a country. Between the years 2005 and 2018, there has been a considerable increase in the number of Facebook and twitter users all over the world. With easy access to social media forums like Facebook, twitter and YouTube, there has been a staggering increase in the number of users over the said forums over the past few years. Capitalising on the outreach of the social media, it was used most effectively to support and propagate the Arab Spring to remove and replace aging dictatorships and monarchies in the Middle East. It is quite well documented that public protests in Tahrir Square in the heart of Cairo in 2011 were mobilized through Facebook.[11]

According to the Pew Research Centre, in USA alone, the percentage engaged with social media usage has increased from a minimum low of 5 per cent in 2005 to a massive 69 per cent in 2018.[12] Among these, the number of female Facebook users outnumber the male users. The numbers have continued to rise ever since. Of the most used social media forums, Facebook has played a distinctive role in gauging public opinion during election season. In this context, facebook users actively took part in the online polls during the elections in the US, UK, Netherlands and even in Pakistan. Considering that a large segment of the potential voters are using Facebook, it is quite evident that electoral managers have used this medium to shape opinions.[13] The perception building company

Cambridge Analytica used the Facebook to harvest data of potential voters to shape public opinion during the US national elections in 2016.

When considering the heightened role and prominence of social media in the realm of mainstream politics and governance, there are two critical dimensions that shouldn't be missed. One, these forums are not just used as means to gauge public opinion but also to significantly alter it. Two, the vital component in the entire social media theatre is 'information'. Valid or not, once a part of the electronic web, the information is shared and re-posted at lengths, to a point that a considerable chunk of the population comes to believe it. The entire exercise results in nothing but often in a blind faith in essentially constructed realities based on distorted facts and misconstrued information. Alongside Facebook, twitter and YouTube have also been used as similar means.[14]

However, the use of twitter and YouTube has been more prone towards dissemination of information and communication unlike Facebook which is mostly equated with the steering of public opinion. As of recently, the use of Twitter by major world leaders to express their views on global developments and most importantly to communicate their foreign policy preferences, has been a common practice. This electronic communication among the leaderships of major countries is a rather new phenomenon, but has resulted in a state of spontaneity whereby the leaders do not necessarily have to conduct meetings in designated spaces to communicate and discuss the issues of national significance. Particularly, twitter remained an important pillar of US President Trump's election campaigning. Even after the assumption of office, Trump has continued to extensively rely on Twitter as a continuum of his aggressive foreign policy rhetoric directed for countries like North Korea, Iran and at times Pakistan. Unhindered use of YouTube and the blogging culture adhered to mostly by politicians and the academic fraternity has further fuelled the dissemination of questionable and unverified information. Information on all sorts of topics is released as a part of video logs and/or private blogs has become a part of the large body of discourse, offering contesting alternative narratives on issues of grave concern for countries, yet without any substantial empirical reasoning.[15]

In case of Pakistan, the paradoxical dilemma of effectively defining the social media spaces, constitution of public opinion itself and the distressing inclination of the public to fall for unverified and unauthenticated news are further multiplied by a notch. In similitude to other major countries, the population in Pakistan, particularly the youth has major inclination and association with an *ad* *nauseam* use of social media websites. On the political front, both twitter and facebook were used as active arenas for political deliberations and communications during the past election. Exchange of rhetoric with other political leaders has also remained a rather glaring feature of the Pakistani politics. As per the statistics collected by the Alpha Pro, a digital marketing firm, there has been an astounding increase in the number of social media users over the past many years. In this view, as of June, 2018, 44.6 million people of the 198.9 million of total Pakistani population are active internet users. And of these 44.6 million internet users, 35.0 million alone actively engage with social media websites. This actually means that of the total population in Pakistan, only 22 per cent has an active access to general internet and of this 22 per cent, 18 per cent uses social media to the extent which can be referred to an active presence on the forum. Intriguingly so, of the 35.0 million active social media users, a massive 92.06 per cent of the masses prefer facebook over a small 4.68 per cent YouTube users and a smaller 1.50 per cent of twitter users.[16] In view of iteration made above, the very fact that most of the Pakistani public, primarily its youth associates more with facebook which is an information sharing forum, than with twitter and/or YouTube which primarily serve the purpose of communication, establishes the critical opening in the realm of responsible information sharing within the country. In case of Pakistan, the entire premise of irresponsible information sharing and the susceptibility to fall for fake news, without necessarily authenticating the source of it, is deeply intertwined with the intricate socio-political and cultural dynamics of the nation from a psychological perspective. The reasons behind adhering to and/or associating with a certain news shared over such forums is deeply rooted in some prior connection of the individual with the subject that the news is about or with the source that which has posted it in the first place. However, in most cases, there is always a self-serving underlying agenda and a deliberate unauthenticated sharing of the online information. As a far-fetched repercussion, this tendency of sharing unverified news has borne deep into one of the defining features of our national character. Above anything else, this tendency is rather detrimental given the fluid nature of information which is half through until the time it has been authenticated at least once. Ironically though, Pakistan stands at least a decade away from instilling among its people a culture of rational and responsible information sharing which takes into account all the long and short term consequences of their actions.[17]

Cyber Attacks

Cyber warfare has increased the asymmetrical threat to a nation's databases and its decision making mechanisms. The threat of cyber-attacks needs immediate attention as nations with considerable resources and more sophisticated informational technology defenses have been compromised by this wave of hybrid warfare. For instance, the attack on over fifteen Iranian facilities and resources by the Stuxnet worm gave its creators access to crucial industrial information as well as giving them the ability to operate various machinery at the individual industrial sites. This introduced a new dimension into the perilous nature of cyber warfare and attacks.[18] However, the unprecedented threats emanating from cyber warfare have led to ventures in countries consolidating more robust security frameworks and Pakistan needs to follow suit.[19] In the case of Pakistan, the technological revolution has made most of digital bases vulnerable. This vulnerability is tested from time to time in the financial, commercial and banking sectors; medical and health services; communication and energy; and national security architectures etc.[20] Keeping in view, the nuanced uses of knowledge and information in the contemporary times, cyber-attacks and information warfare poses dangers to national security that is more profound than conventional threats. For instance, in November, 2018, data from "almost all" the banks in Pakistan was compromised in a cyber-attack and extensive amount of money was stolen from many accounts as the security system was breached. [21] This attack came to light after a few days of another attack on the Pakistani banking security infrastructure where Bank Islami Pakistan reported that it had been a victim of theft of almost 3 million rupees.[22] Repeated and consistent attacks to the national wealth of the state need to prompt a more robust policy and practical response to bolster the security systems and infrastructure of the state. It goes without saying that another precious data base of a country is the concerning armed forces in the country which are also open to attacks. There are persistent threats to breach these data bases.

Incontrovertibly, the nature of warfare has shifted from physical to online threats; the new cyber arsenal disguises itself as state sponsored attacks, disinformation and espionage. This transformed threat cannot be addressed with conventional and customary responses, but needs to be approached with accelerated development of innovative cyber and information strategies, regulatory frameworks, common standards and tangible capabilities all aimed at achieving a harmonized regime to counter cyber warfare.

Psychological Manoeuvring; Targeting the National Will

The most distressing feature of hybrid wars and the one that adds manifold to the challenge of effectively deterring them is the damage that it causes on the psychological level. As discussed earlier, a kinder form of war that it is, the impact that the strategies deployed under this stream of warfare are twice as severe in their tenacity. The information-centric component within the hybrid warfare doctrine targets the very spirit of the adversary country. Information based wars have the potential to influence political, economic or military goals at any and all levels. They can sabotage the economy, development ventures, and/ or the sabotage or destruction of the entire information network system. It essentially includes collection of tactical information, deliberately spreading propaganda and disinformation to demoralize or manipulate the adversary.[23] Endless debates over electronic media citing the inadequacy in the policy and governance structures within lead to a state of conditioning nations into believing in the inability of their national leaders to lead their countries into the rightful direction. It must be noted that like other forms of hybrid warfare, the linchpin of psychologically tarnishing the very spirit of nations lies in 'information', its unverified release and sharing. It must also be noted that for the advancement of such an agenda, it does not necessarily have to be an external source to act as a carrier of fake news. In case of Pakistan, there is a lot that needs to be done on this front. At present, varying discourses in the electronic, print and social media regarding Pakistan's engagement with the multi-billion dollar deal CPEC is one such example. The doubts about the longevity and credibility about the engagement began on a similar note and have now grown into a daily dose of debate as to whether the alliance is a good idea or not.

Policy Options

There is an urgent need to understand and address the multi-faceted threat posed by hybrid warfare. Due to the heightened susceptibility to fall victim to these stratagems, national security paradigm needs to be overhauled.[24] There is a clear cut need to devise a strategy, build capacities and allocate resources. The response should be a whole of government approach and the people should be made a part of it. Operating in silos and turf rivalry can only increase the threat and not decrease it. Recommended options are as under:

- First and foremost, there is a need to create awareness among our top level policy and decision makers about the need to register and recognize hybrid warfare as the contemporary currency of war and to come up with an imaginative counter strategy. Notwithstanding the fact that there should be an integrated and holistic approach to synergise all resources (civil and military), there is no harm to make one of the ministries the lead agency. This ministry can be officially mandated to develop a national narrative to counter false claims of disunity or worse disintegration. Innovative themes can be constructed to produce a positive ambience and raise the morale of the nation. The person responsible for this effort should be answerable to the Prime Minister and should regularly update the Parliament and where needed the nation. This person should also be provided adequate financial, material and human resources to plan and fight a meaningful battle to counter hybrid threats.

- Secondly there is a need to make a clear cut policy integrating all the civil and military agencies to come up with a sustainable model. The government can achieve this by engaging all the stakeholders within the society in the formulation of an altogether new security paradigm. In this view, practically viable means to lessen the vulnerability in the cyber realm must be made part of the country's national security doctrine. The military can be asked to revise its threat hypothesis to cover all aspects of the hybrid threat. Inputs from noted economists, academics, cyber war experts, scientists and law enforcement agents can be factored into formulating the new threat dimensions.
- Thirdly, at the foreign policy level, alliances should be sought with friendly countries to strengthen our digital defences. International best practices must be introduced with the help of partner countries and organizations to achieve the gold standard in cyber security. Universities should be encouraged to come up with policies and technologies to secure our cyber and mental frontiers.
- Fourthly, investment should be made in human resource. Young university students and fresh graduates in the market with the knack of fighting cyber warfare in the domain of not only science and technology but also in hard core information warfare should be hired. They should be trained to work in small teams to counter various facets of the hybrid threats.
- Fifthly, serious planning should be done to manufacture our own hardware and software. Currently all computers, laptops, smartphones and servers are imported. None of our data bases are running on machinery produced by our own technologists. Similarly all our operating systems are those produced by companies such as Microsoft. We do not have any digital search engine of our own. Our universities submit all their intellectual outputs to similarity index software such as Turnitin. This can only perpetuate intellectual hegemony of the West. None of our thoughts and research belongs to us. It is captured by software produced externally.
- Last but not the least, Pakistan must energize its defensive information mechanism on state and social media to spread competing narratives to fight gloom and doom stories.[25] This is easier said than done, it will need a

lot of imagination and foresight to develop positive themes to raise the national spirit and morale and nip the negative broadcasts in the bud.

Conclusion

Wars have always been waged with all the tools available to a nation (financial, political and diplomatic) to achieve a political goal. A weak nation remains always at the mercy of a stronger adversary. This does not only mean just having a top class military outfitted with latest weapons of war but a strong and resilient nation willing to undergo all sorts of trials and tribulations in order to survive at its own terms. This means essentially that the nation should be at peace with itself. It should believe in its leadership and the capacity and capability of the state institutions to function for its good. Common man must have two square meals a day and a roof over his/her head. The children must be in schools and not out on the streets begging. There should be access to quick and fair justice. There should be hospitals for the sick, water in the taps, gas in the pipelines and the bulbs must light up after dusk. The state should be sympathetic towards its citizens and in a position to look after the needy. The police should protect the citizens from the criminals and the army should be able to defend the borders.

In such a state of satisfaction and contentment, hybrid threats would be ineffective. Such threats can only thrive if the people are unhappy or they perceive that the government is either incapable or worse unwilling to provide them or a certain segment of society their due share as the responsible citizens of the country. If their basic human needs are fulfilled they will not fall prey to malicious propaganda and no amount of canvassing would convince that a collapse is imminent any time soon.

To prevent any worst case scenario from happening not only a positive narrative needs to be created but also all national policies should be made on the basic principles of being people friendly and welfare oriented. Physical frontiers can be defended but collapse on the mental front can lead to surrender without fighting. This must be prevented come what may and the national will and spirit must be protected at all costs.

NOTES

[1] Frank G. Hoffman, “Conflict in the 21st Century: The Rise of Hybrid Wars”, (Arlington: Virginia, 2007), 7-10, accessed August 6, 2018, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[2] Patrick J. Cullen and Erik Reichborn-Kjennerud, “Understanding Hybrid Warfare: A Multinational Capability Development Campaign Project,” January 2017, Accessed December 31,2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

[3] Timothy B. McCulloh, “Understanding Hybrid Warfare and Gray Zone Threats,” in *Terrorism: Commentary on Security Documents - Hybrid Warfare and the Gray-Zone Threats*, ed. Douglas C. Lovelace, Jr., (New York: Oxford University Press, 2016), 59-65.

[4] Peter R. Mansoor, “Introduction: Hybrid Warfare in History” in *Hybrid Warfare- Fighting Complex Opponents from Ancient Worlds to the Present*, ed. Williamson Murray and Peter R. Mansoor (USA: Cambridge University Press, 2012), 1-15.

[5] James K. Wither, “Making Sense of Hybrid Warfare”, *Connections* 15, no.2, (2016): 74-78.

[6] Brian Nichiporuk, “U.S: Military Opportunities: Information-Warfare Concepts of Operation” in *Strategic Appraisal: The Changing Role on Information Warfare*, ed. Zalmay K., White J.O., and Marshall A W (Santa Monica: RAND Corporation, 1999): 187-195.

[7] Saghir Iqbal, “Hybrid Warfare and its Impact on Pakistan’s Security”, (CreateSpace Independent Publishing Platform, 2018):5-13.

[8] Hafeez ullah Khan and Ijaz Khalid, “Indian Cold Start Doctrine: Pakistan’s Response,” *Journal of Research Society of Pakistan* 55, no.1 (2018): 325-341.

[9] *Uri: The Surgical Strike* Imdb (2019), https://www.imdb.com/title/tt8291224/ .

[10] Shireen M. Mazari, “Hybrid Warfare and Centre of Gravity,” *The News*, December 27, 2018, https://www.thenews.com.pk/print/411092-hybrid-warfare-and-centre-of-gravity (accessed January 7, 2019).

[11] Zeynep Tufekci and Christopher Wilson, “Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square,” *Journal of Communication* 62, no.2, (2012):363-379.

[12] “Social Media Fact Sheet”, *Pew Research Centre*, http://www.pewinternet.org/fact-sheet/social-media/ (Accessed December 27' 2018).

[13] Nick Anstead and Ben O’ Loughlin, “Social Media Analysis and Public Opinion: The 2010 UK General Election,” *Journal of Computer-Mediated Communication* 20, (2015):204-210.

[14] Robin Effing, Jos van Hillegersberg and Theo Huibers, “Social Media and Political Participation: Are Facebook, Twitter and YouTube Democratizing Our Political Systems?” *Department of Information Systems & Change Management, University of Twente, School of Management and Governance,* (2011): 25-29.

[15] Rebecca Rabby et al., “Vlogging on YouTube: the online, political engagement of young Canadians advocating for social change,” *Journal of Youth Studies* 21, no.4, (2018):495-509.

[16] “Pakistan Social Media Stats 2018, http://alphapro.pk/pakistan-social-media-stats-2018/ (Accessed January 2, 2019).

[17] Hamid Bilal, *Consultant Psychologist, Compass Training and Consultancy Pvt. Ltd.* (Interviewed January 3, 2019).

[18] Michael Holloway, *Stuxnet Worm Attack on Iranian Nuclear Facilities.* July 15, 2015, http://large.stanford.edu/courses/2015/ph241/holloway1/ (Accessed January 01, 2019).

[19] Kate O'Flaherty, *Cyber Warfare: The Threat From Nation States*, Accessed January 01, 2019, https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#3d35c84f1c78

[14] Farooq Baloch and Iftikhar Firdous, *Pakistani banks hit by biggest cyber-attack in country’s history*, https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/ (Accessed January 01, 2019).

[21] Shakeel Qarar, 'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head. Accessed January 01, 2019, https://www.dawn.com/news/1443970

[22] Salman Siddiqui, Pakistan's banking system witnesses another cyberattack. Accessed January 01, 2019, https://tribune.com.pk/story/1836466/2-pakistans-banking-system-witnesses-another-cyberattack/.

[23] Dragan Z. Damjanović, “Types of Information Warfare and Examples of Malicious Programs of Information Warfare”, *Military Technical Courier* 65, no.4 (2017): 1044-1053. http://dx.doi.org/10.5937/vojtehg65-13590

[24] Andrew Korybko, “Applicability of Hybrid Wars to Pakistan: Challenges and Possible Responses”, *NDU Journal* XXXI, (2017): 207-228. http://www.ndu.edu.pk/issra/issra_pub/articles/ndu-journal/NDU-Journal-2017/Journal_2017.pdf

[25] Sehar Kamran, “Hybrid Warfare- Emerging Challenges for Pakistan”, *The Nation,* April 29, 2018. https://nation.com.pk/29-Apr-2018/592255 (Accessed December 27, 2018).