No. – 7 – 2017

USI Occasional Paper

New Threats in the Information Warfare Domain

Col Anurag Dwivedi, Senior Research Fellow, USI

Introduction

Warfare is as old as civilisation itself and the destiny of empires have coincided with victories or defeats. While war has remained a near constant of human existence, the 'methods' of waging war have constantly evolved due to tactical or technological '*innovation*'. Understood and applied correctly in terms of strategy and operational doctrine, innovations have invariably surprised the enemy and proved decisive to outcomes.

Not all innovations have a technological foundation. Introduction of 'war elephants' by ancient Indians and their subsequent adoption by the Persians and Alexander around 330 BC is one such example of non-technical innovation. Guerilla warfare is yet another tactical innovation whose history can be traced back to Sun Tzu (600BC). Terrorism and insurgency are its modern tactical avatars. That said, the most transformational changes brought about in war fighting, at least in modern times, can be attributed to scientific and technological innovation. Changes to operational doctrine and tactics have followed suit. The invention of Submarines (1863), Airplane (1903), Tanks (1915) and Nuclear Weapons (1945) are notable examples where scientific and technological innovations have resulted in a profound impact on operational doctrine and even strategy.

> The most transformational changes in modern war fighting can be attributed to scientific and technological innovation. Changes to operational doctrine and tactics have followed suit.

It must also be remembered that none of the aforementioned scientific or technological innovations were abrupt developments. Each one of them took years of refinement before they attained critical mass and were effectively fielded in war. It took several more years before operational doctrines and tactics matured to the extent of becoming common parlance, practice, and training. The first tanks, for example, were employed during World War I but they fully came into reckoning only during World War II and the new operational doctrine of Blitzkrieg was born. The doctrine of Mutually Assured Destruction (MAD) likewise matured after the first nuclear bombs were dropped on Japan.

An instructive example is that of the Machine Gun. Machine guns underwent evolution and development for over 300 years before technology reached an inflection point and the United States army issued four machine guns per regiment in 1914. This increased to 36 machine guns per regiment by 1918 - a rapid adoption by any yardstick[i]. Even more dramatic is the case of fighter aircraft. The first successful controlled flight of a fixed wing aircraft was demonstrated by Wright brothers in December 1903. Less than two decades later more than 50,000 airmen had died in combat during World War I[ii]. Three decades later, World War II saw the most extensive use of airpower in the history of warfare and 'Air' came into being as a distinct battle space. Similar is the story of Submarines, the Tank, and Nuclear weapons. Technology got rapidly inducted once it reached an inflection point and thereafter played a pivotal role in all future battles. Tactics, doctrine, equipment, and strategy were suitably renewed.

Col Anurag Dwivedi, is Senior Research Fellow at the United Service Institution of India.

A key indicator of technology induced doctrinal shift is, therefore, that it results in a manifest change in the equipment holding as well as organisation profile of the armed forces. Secondly, it results in creation of new manpower specialties that hitherto fore did not exist,viz, fighter pilots. Lastly, doctrinal shift is visible in the form of rapid adoption of offensive and defensive counter-measures,viz, Anti-Submarine, Anti-Aircraft, and Anti-Tank warfare.

An even more profound transformation is signalled when an entire new battle space opens up. 'Land' and 'Sea' were the two ancient battlespaces. These were joined by 'Air' during the World Wars and from 1970s onwards 'Space' became a fourth battlespace. The latest addition to this list of battlespaces is 'Information'. Today Land, Sea, Air, Space, and Information (which includes Cyber) are the five deemed battle spaces where firepower, manoeuvre, control, agility, and awareness are to be applied.

It is also interesting to note that submarines, tanks, fighter aircraft, and nuclear weapons did not result in the other one going obsolete. Over a short cycle, lasting few decades, multiple transformational innovations co-exist and get employed in complementary fashion, though the new one may gain increasing prominence. Operational doctrine gets overhauled after each such transformational induction and tactics and equipment design are suitably altered to adapt to the new paradigm. When we look at longer time cycles however, the war elephants as also the horse cavalry and archers actually did become obsolete.

A key indicator of technology induced doctrinal shift is that it results in changes to organisation, equipment profile and manpower specialities. The most profound transformation in war fighting is signalled when an entire new battlespace opens up.

Network Centric Warfare

More recently, Information and Communication Technology (ICT) has ushered in a similar doctrinal shift. ICT, as an innovation, followed a trajectory of rapid adoption from 1980s onwards once it reached inflection point. Numerous old weapon platforms and equipment got replaced by a new generation of equipment that is software controlled and embedded with microchips, sensors, and communication. The Information Technology (IT) specialist has become a common and indispensable trade specialization found in every Headquarter and military establishment. The extent of adoption can be gauged from the fact that, even the humble infantry soldier is now envisaged to be equipped with devices which can compute and communicate. The main virtue of this ICT enabled generation of battle platforms is their ability to integrate, generate, and assimilate information thus enabling synchronized application of combat power beyond visual range. The resultant new doctrine is now commonly termed Network Centric Warfare (NCW).

NCW is slightly difficult to comprehend because it is not uniquely identifiable with any specific weapon platform. Instead, it relies on creation of a force multiplier effect by synchronizing combat power of geographically dispersed forces through shared situational awareness and better command and control. A scaled down example that can help understand this concept better is the famous doctrine of Blitzkrieg. Blitzkrieg was to a large extent attributable to a simple innovation by Heinz Guderian of fitting each German tank with a wireless set[iii]. The resultant situational awareness and improved command and control enabled the German Panzer Divisions to extract far greater combat potential from their tanks and outmanoeuvre adversaries having similar platforms.

Just like aircraft and aviation, the transformational utility of ICT was so profound that it also rapidly proliferated in the civilian domain resulting in the advent of the 'Information Age'.

Information – Understanding the New BattleSpace

This preamble of ICT and NCW is essential to place 'information' as a battlespace in its proper context. Bits and bytes are the bullets of this new battlespace and just like manufacturing and firing of bullets would have rapidly multiplied coinciding with proliferation of machine guns; the quantum of information generated (manufactured) and transmitted (fired), rapidly multiplied coinciding with the advent of NCW and the Information Age.

Each battlespace has certain unique characteristics which is why land warfare, sea warfare, and air warfare are distinct from each other though complementary. When it comes to Information as a battlespace, the uniqueness lies in its all-pervasive and ubiquitous nature. Unlike battleships and fighter jets, the armed forces don't have monopoly over production, possession or operational employment of information. Nor is there a distinct dividing line between military and civilian information. Instead, it is a complex, all-encompassing battlespace open not just to armed forces but also to civilian enterprises, quasi-military professionals, hackers, geeks, non-state actors, and terrorist organisations. This environment is also sometimes called the 'Infosphere'[iv].

As mentioned earlier, every major innovation resulted in a rapid adoption of offensive and defensive countermeasures. The advent of tanks, for example, resulted in adoption of anti-tank weapons (offensive) and ditch cum bunds (defensive). Anti-submarine and anti-aircraft measures likewise became specialized disciplines in themselves. Once 'information' became the latest enabler of NCW, it was but logical that anti-information measures would also come into existence.

> The uniqueness of "Information" as a battlespace lies in its all-pervasive and ubiquitous nature. Just like dogfights that happen in aerial combat; similarly an Information vs Information fight take place in the Infosphere.

Lastly, like any other battlespace – there is a struggle for dominance or superiority that takes place within it. Just like ships and submarines battle it out at sea or dogfights that happen in aerial combat – similarly there is an 'Information vs Information' fight that takes place within the Infosphere to gain decisive information superiority or at least a favourable information edge.

This war involving Information and which takes place in the Infosphere is called Information Warfare and can be broadly divided into two sub-classes namely, anti-information (creating uncertainty) and information vs information (information dominance).

Information Warfare (IW)

Military strategists in particular have been repeatedly blindsided by the irreversible momentum gained by the ICT transformation and the resultant rise of IW. IW can today be said to have superseded NCW or subsumed it into a larger doctrine depending on whether one believes it to have attained critical mass as yet or not.

Just like NCW, IW is tangibly different form earlier revolutions in military affairs. There are no specific weapon systems or platforms associated with IW. Information Warfare also does not involve any direct transaction of kinetic energy and firepower. The intangible nature of IW can be understood by using the analogy of digital currency versus printed banknotes. If the aim is to achieve a financial transaction, both forms can achieve the objective. Also, while cash is more useful for buying snacks from a roadside stall, the digital version is more effective for online purchase of a rail ticket – hence IW and kinetic weapons co-exist. As Deng Xiaoping said - "It doesn't matter whether a cat is white or black, as long as it catches mice."

Consider a hypothetical example wherein the strategic war objective is to bring about a favourable regime change in another country. The Kinetic Energy method was operation Iraqi Freedom. Its IW equivalent is the alleged hacking of US Presidential election by Russians. Both achieved the desired regime change and the latter did so with much greater sophistication and deniability. Likewise, if the stated aim is to destabilise a region - the social media fuelled insurgency has recently achieved in Kashmir what conventional infiltration and cross-border support was failing to accomplish for several years[v]. The Islamic State is yet another example of how IW is being leveraged to wage a Fourth Generation War on a global scale.

It is worth citing few more examples besides the much publicised Russian hacking to influence US Presidential elections and the social media fuelled global jihad of ISIS. In 2010, the Stuxnet worm penetrated and caused a major setback to the Iranian nuclear program. In 2013 Edward Snowden copied and revealed highly classified data from the US National Security Agency (NSA) thereby compromising ongoing and future operations. In 2016, classified documents pertaining to the Scorpene submarines being supplied to India by French firm DCNS were leaked. The common threads that can be discerned are:-

- Information or information based systems were exploited in all cases
- No Kinetic weapons were employed
- The targets were all highly secure
- All actions resulted in strategic losses to the target
- The aggressor was identified only post-strike or remained elusive

Till a few years ago, IW and its primary affiliated domains of Electronic Warfare, Cyber Warfare, and Psychological Operations were used much like preparatory bombing to destabilize the enemy before the tanks and infantry rolled in. We are now witnessing a shift wherein, Information Operations by themselves achieve strategic objectives without relying on armed conflict. This has a profound bearing on operational doctrines and force structures.

Sun Tzu had famously said, "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill". Such is the growing power of IW.

Till few years ago IW was used much like preparatory bombing to destabilise the enemy. We are now witnessing a shift wherein Information Operations achieve strategic objectives by themselves, without relying on kinetic engagement.

With that in mind, it would be worth looking at some latest additions in the IW arsenal that will further enhance its lethality and make it the dominant form of future conflict.

New Threats in the Information Warfare Domain

➢ The Rise of Internet and Social Media

It would not be inappropriate to state that the Internet in general and social media in particular has become a playground of IW and an instrument for waging covert war by other means. The emerging threats are summarised below:-

- The Internet has enabled a unique decentralized command and control model that is faceless and independent of geographical boundaries. Many conventional strategists for example have been flummoxed by the lack of direct leadership in uprisings like those that took place 2010 onwards during the Arab Spring or the latest episode in Kashmir. A typical case of searching for the wrong thing in the wrong place. The leadership in the Information Age has actually migrated to the Internet and need no more be present on ground. It may well exist in the form of a 'WhatsApp' group. Terrorist organisations, like ISIS, are some of the most prolific users of Internet for multitude of functions like recruiting, motivating, finance, and training.

- Social media has become a factory of revolutions. While governments and leaders are increasingly using it, they are also being increasingly blindsided by sudden online developments. The videos uploaded on social media by few Indian paramilitary and army soldiers is one such recent example which disrupted existing narratives and forced the political and security establishment to hastily react. Leaders (and by proxy their nations) are increasingly being pushed into crisis mode by disruptive data or clandestine audio/video recordings leaked on Internet by anonymous individuals and thereafter mass circulated over social media. This is the new normal.

- Crowd sourcing is another Internet based phenomenon with military implications. No secret service has been able to accumulate and deploy intelligence with such destructive effect as Wikileaks, which is essentially a crowd sourced intelligence agency. Satellite imagery and cartographic data used to be classified military matter before Google came out with Google Maps, Earth, and Street View. In 2013, Google added crowd sourcing to Street View[iv]. Tracking devices that allow objects to be tracked in real time using either (or a combination of) GPS, Bluetooth and Internet have become extremely small and cheap. 'Crowd GPS', where button size tracking devices can be attached to objects and a smartphone

equipped user community uploads location data whenever they pass by a tagged object, is another unique example[vii]. Using such techniques, it is literally child's play to track movement of military commanders and convoys over Internet without taking any overt risk. The 'Internet of Things' is the next big step in this revolution.

- Fake news is yet another threat gaining in magnitude to the extent that Mr Donald Trump, the new President of the United States has labelled conventional media as lying and dishonest. The Fourth Estate is losing credibility with common masses as well and it is fairly common to hear the phrase 'paid media' in daily conversations. Social media has filled the vacuum. Content generation and opinion shaping is now being done by millions of bloggers, Facebook, Twitter, and WhatsApp users – the ultimate combination of crowdsourcing and anonymity. This, in turn, has led to the phenomenon of professionally designed fake news. Such has been the spurt in fake news that recently one such article prompted the Pakistani defence minister to threaten nuclear retaliation against Israel[viii].

The ability of Internet and Social Media to manipulate a nation's government and the will of its people has far greater strategic impact than mere hacking.

In a larger perspective, the disruptive power of Internet and social media has given an extremely potent tool to the non-state actor while the nation state has become increasingly vulnerable to losing control of narrative and public sentiment. This ability of Internet and social media to manipulate a nation's government and the will of its people has far greater strategic impact than mere hacking. This is a major new facet of IW.

➢ Software as an Agent and Software as a Weapon

Many of our IW constructs still revolve around traditional computers and so called cyber security. The traditional concepts, however, no longer apply. The fact is that computers have evolved and now also come disguised as smartphones or telephone exchanges or ATM machines. They are even embedded inside cars and aircraft and an increasingly large number of industrial machinery and household electronics. The embedded software and app based eco-system is yet another IW hotbed.

- In November 2016, US security firm, Kryptowire, discovered that a secret software which came preinstalled on low cost Android smartphones was transmitting full contents of text messages, contact lists, call logs, location information and other data to a Chinese server every 72 hours without user consent or knowledge. The Chinese firm that wrote the software, Shanghai Adups Technology Company, says its code runs on more than 700 million phones, cars, and other smart devices and that it intentionally designed the software to help a Chinese phone manufacturer monitor user behaviour. According to the report, Adups provides software to two of the largest cell phone manufacturers in the world, ZTE and Huawei[ix]. The justification sounds deceptively similar to Google, Facebook, WhatsApp and many others. Private information is the currency in which we pay for seemingly free services like Search Engines and Messengers. In March 2016, three rogue apps called WeChat, Smesh, and Line were blacklisted in India because they were transmitting sensitive user data to Pakistan. Serving and retired Indian military personnel were specifically lured to install the app via honey traps set up by ISI on social media[x]. Honey traps used to be a classic espionage technique which now is increasingly being adapted to the virtual world and being combined with cyber exploits. This is as close as one gets to confirmed intelligence from a highly reliable source. Any trained Electronic or Cyber Warfare specialist worth his salt would be able to compile identity of

units, names, and profile of Commanders, geographical locations including movement of troops, administrative routines, state of morale and preparedness with just a few such compromised smartphones (or software apps) existing in a field formation. No apparent breach of conventional Cyber Security protocols and SOPs would be noticed and no rogue agents discovered. It is also not possible to prohibit these devices. At best, they can be deposited outside ops rooms or sensitive premises, but that changes nothing. In fact a few hundred smartphones converging for three hours at a specific location is in itself valuable information.

- Hacking of "Smart" devices like TVs, webcams, home thermostats, remote power outlets, sprinklers and automatic door locks have already been demonstrated in various Black Hat events[xi]. In 2015, researchers Charlie Miller and Chris Valasek demonstrated their abilities to control a Jeep Cherokee remotely from miles away by exploiting the car's entertainment system that was connected to the mobile data network. They were able to move laterally into other electronic parts of the vehicle, like the air conditioning, transmission, and even the car's steering controls[xii]. Driverless vehicles are soon supposed to become a reality. Attacks using vehicles like the one in Nice or truck bombs may no longer require a terrorist behind the wheels.

- In the 2013, at Hack in the Box conference in Amsterdam, security consultant Hugo Teso demonstrated an App, called PlaneSploit, wherein he could take control of a commercial airplane remotely without needing physical access to the aircraft. Theoretically the hacker could command the plane using an Android phone[xiii]. More such exploits including leveraging a plane's onboard Wi-Fi signal or in-flight entertainment system to hack into its avionics equipment have been reported. And, we know well how the war in Afghanistan started.

It will not be incorrect to conclude that the age of 'Software as an Agent' is already thriving and the age of 'Software as a Weapon' is about to commence. This is a transformational new facet of IW.

➢ A Wireless Future

- One important lesson still taught in basic military training is about Electronic Emission Policy (EEP). The most secure means of communication is supposed to be line, followed by microwave and radio. Wireless radio is supposed to be opened only when other primary means of communication get disrupted or in an emergency. The information age has disturbed this status. The need to be continuously connected on the move has meant that wireless has become the primary means of communication and networking. Bandwidth limitations have largely been overcome with new technologies like 4G LTE. Whole cities are becoming Wi-Fi enabled and mobile networks have proliferated in border areas. The boundaries between civil and military communications have also become somewhat blurred as we see most soldiers carrying smartphones even in field areas.

The need to be continuously connected has led to wireless becoming the primary means of communication and networking. Electronic Warfare comes into play in a major way.

- Even on the battlefield, proliferation of sensors and UAVs has resulted in a growing reliance on radiating media. Space based assets obviously depend totally on radiated frequencies for command, control, telemetry and data transmission. Future Soldier projects of various countries invariably include a wireless radio transmitter as part of the combat gear. All Global Navigation Satellite Systems (GNSS) are wireless. The future may also see robots and autonomous machines on the battlefield which would again rely on wireless communications.

- This inevitable saturation of our environment, including the battlefield, with wireless communications is yet another new threat. Electronic Warfare comes into play in a big way, including targeting space based assets. A new form of warfare, called Navigation Warfare (denial of GNSS), is already taking shape and as a consequence, the US Navy reintroduced celestial navigation training after a gap of 15 years in 2015[xiv]. Directed Energy Weapons (DEW) may also become a game changer.

➢ Critical Information Infrastructure

- The concept of 'Critical Infrastructure' is now well enshrined in national security doctrines of many countries including India. Defence, Telecommunication, Financial Services, Energy, and Transport sectors typically comprise the critical infrastructure. Inevitable reliance on a network of electronic devices and software that communicate over cable or wireless (collectively termed as the Critical Information Infrastructure) has made them extremely vulnerable to cyber and electronic attacks.

> It can be stated with near certainty that any future war will start with a massive assault on the critical information infrastructure.

- Information operations have been used as a precursor to conventional operations in past wars as well but the quantum of threat has evolved and grown exponentially. Electronic attacks against communication networks have a long history but it was during Operation Desert Storm that Electronic Attacks were used to neutralize not only the communications but also the Iraqi Air Defence Systems[xv]. Cyber-attacks came into play thereafter and government websites and Internet infrastructure was specifically targeted during the 2008 Russo Georgian war[xvi]. Since then, there have been increasing instances of electrical grids, financial systems, telecomn networks and other critical infrastructure being systematically targeted by both state and non-state actors[xvii], [xviii].

- With increasing dependence of critical infrastructure on ICT, it can be stated with near certainty that any future war will start with a massive assault on the critical infrastructure and it will have a devastating effect.

Conclusion

There still remain some sceptics who do not see IW as the dominant form of future warfare or restrict it to hackers gaining control of computers by exploiting password and software vulnerabilities or via malicious software installed through infected USB pen drives or clicking on bad e-mail attachments. As explained in this paper, IW is a far larger canvas and a much larger construct manifesting across the entire spectrum of conflict from the strategic to the tactical. Plausible deniability, combined with absence of agreed Laws of War and Treaties makes IW as the first choice for offensive operations by both state and non-state actors.

Most modern armies have recognised IW as an independent way of waging war similar to land, sea, or air warfare. The latest developments outlined here are likely to further improve its lethality wherein, it may be used independently or in tandem with conventional firepower to achieve strategic objectives. Beyond this looming inflection point, IW will, out of sheer utility and necessity, become the dominant form of warfare and dramatically transform the role, operational doctrine and organisation of armed forces.

End Notes

i. http://www.1914-1918.net/mgc.htm. Accessed on 01 February 2017
ii. John Buckley (1998). "Air Power in the Age of Total War". Taylor & Francis.
iii. Guderian, Heinz (2001) [1952]. Panzer Leader. New York: Da Capo Press
iv. https://en.wikipedia.org/wiki/Infosphere. Accessed on 20 Jan 2017
v. Making of a social-media militant. The Telegraph, 11 July 2016
vi. https://maps.googleblog.com/2013/12/create-your-own-street-view.html. Accessed on 23 Jan 2017
vii. http://support.thetrackr.com/hc/en-us/articles/204687875-What-is-Crowd-GPS-. Accessed on 23 Jan 2017
viii. Reading Fake News, Pakistani Minister Directs Nuclear Threat at Israel. The New York Times, 24 Dec 2016
xi. https://krebsonsecurity.com/2016/11/chinese-iot-firm-siphoned-text-messages-call-records/#more-36939. Accessed on 23 Jan 2017
x. http://www.news18.com/news/india/army-blacklists-3-apps-warns-troops-against-using-wechat-smesh-lime-1216356.html. Accessed on 23 Jan 2017
xi. http://www.cbsnews.com/news/black-hat-2014-cybersecurity-experts-hack-home-alarms-smart-cars-and-more/. Accessed on 10 Jan 2017
xii. http://thehackernews.com/2015/07/car-hacking-jeep.html. Accessed on 10 Jan 2017
xiii. https://www.bloomberg.com/news/articles/2013-04-12/hacking-an-airplane-with-only-an-android-phone. Accessed on 10 Jan 2017
xiv. http://www.navy.mil/submit/display.asp?story_id=91555. Accessed on 11 Jan 2017
xv. Kopp Carlo, "Operation Desert Storm :The Electronic Battle, Parts 1 – 3" (Australian Aviation, June/July/August, 1993)
xvi. Hollis David, "Cyberwar Case Study: Georgia 2008" (Small Wars Journal, 2010)
xvii. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm. Accessed 20 Jan 2017
xviii. https://en.wikipedia.org/wiki/Cyberwarfare#Types_of_threat. Accessed on 20 Jan 2017

Price: ₹ 100.00 / US $ 1.95

United Service Institution of India (USI)

Rao Tula Ram Marg, Opposite Signals Enclave, New Delhi-110057
Tele: 26146774/ Fax: 26149773, E-mail: cs3@usiofindia.org