Book Review

Future of War

Anurag Sharma

Dr Robert H. Latiff, Future War:
Preparing for the New Global Battlefield,
First Edition, Knopf Publishing House, 2017,

A quick look at the cover of Robert Latiff's *Future War: Preparing for the new global battlefield*, can be a little misleading as it seems to be a fictional work. It shows a shadow of a gunman falling over an integrated circuit board. However, the book is a serious work that explores how futuristic technology is changing warfare and the security environment. Dramatic developments in dual use and military technology pose challenges to both soldiers as well as policymakers. At the same time, the book also takes the reader to the research labs where experiments on the inter-disciplinary areas, such as biologically enhanced warriors, cyber-enabled weapons, which are in the process of becoming reality.

New and even 'future' technologies are sweeping into weapon systems and dramatically remaking the battlefield in the 21st Century. A 'Future technology' could be referred as a 'hypothetical technology' which do not exist at present, but could exist in the near future. The introductory chapter opens with several US-centric hypothetical scenarios in which major powers such as US, China and Russia are in tense relations over the South China Sea, Russia's involvement in Ukraine and Syria. A sudden change in the operational behaviour of automatic turbine motors due to a computer malware can be seen, and somewhere else a group of elite commandos of an unidentified national army—

Anurag Sharma, Research Associate, VIF

equipped with high-technology driven weapons, are ready to attack US and its interests. Such hypothetical scenarios is nothing but a preview of a 'futuristic' war.

The author recalls the post-September 11 attack environment in US, where everyone was calling out to avenge the drastic terrorist attack. Following the National Emergency declared by the then US President George W. Bush, the author issued orders to call the reservists to active duty and extending the active duties of those whose tours were due to end. The author points to the statement made by Chinese colonels—Qiao Liang, and Wang Xiangsui in 1999, when they predicted how the future battlefield would look like:

> *"Soldiers would be computer hackers, financiers, and agents of private corporations rather than the members of a regular army. Their weapons would not only consists of airplanes, cannons, biological or chemical bombs but also enabled of computer viruses, Internet browsers, and financial derivative tools."*[i]

The use of Stuxnet virus against Iran, is one of the good examples where technology was used as a weapon by State(s) against a State. In 2010, the US and Israel (never claimed), used 'Stuxnet' computer virus to break Iranian nuclear centrifuge equipment, which is used to produce uranium to empower the nuclear weapon and reactor. Stuxnet— a sophisticated virus, exploits the vulnerabilities of a Windows-based computer systems and then spreads through the network.

The author traces his journey from graduating with a PhD in Engineering and his transfer from US Army to Air Force, where he learned about the upcoming technologies for a new generation of stealth aircrafts. The author's last professional assignment was at the National Reconnaissance Office (NRO) where US spy satellites are designed, built and tested for operations. His task included watching and listening to the adversaries and working on joint projects with other intelligence agencies and government organisations such as the Central Intelligence Agency (CIA), National Security Agency (NSA), and the Department of Defense (DoD). Everything --be it conventional bombs, communication equipment, satellites, advanced armour systems, and navigation systems – today are dependent on computer and its components. Talking of surveillance, Latiff says that in 2002 the video surveillance industry was worth USD 2 billion, whereas it reached USD 21 billion by 2015. The emerging technologies like Automated Identification Software (AIS), face and eye scans, Radio-Frequency Identification (RFIDs) tag, etc., collect human data on a large scale. The massive data collection are a boon for the law-enforcement

---

Robert D. Latiff, Future War: Preparing for the new global battlefield. New York: Alfer A. Knopf, 2017, p.4

agencies. However, the Internet of Things and Wifi-enabled devices, which have 'always-on' sensors, are a threat to privacy.

Even though the world still does not completely comprehend the use and impact of technologies such as Artificial Intelligence (AI) and synthetic biology, still they will be used as or part of weapons in near-future warfare. On synthetic biology, author describes his conversation with Dr Justin Sanchez, Director of the Defense Advanced Research Project Agency (DARPA)'s Biological Technologies Office (BTO). The BTO's research on the biological measures for the protection of an individual soldier includes an exploration of complex biological issues that will enhance the ability of soldiers to engage in warfare and to recover from injuries. A neuroscience technology would help in the recovery of a wounded soldier from a traumatic brain injury. Research was also on to implant a chip to restore the brain functioning and the peripheral nervous system. Dr Sanchez assured the author that the research is for defensive purposes but could be used for offence as well. Biologically enhanced soldiers could be faster, stronger and smarter, but the experiment could also make him an emotion-less brutal warrior. There is a point of disagreement on re-programming the brain functioning of a wounded soldier. Deleting a traumatic memory or re-programming his brain would be an intrusion in the personal integrity of the soldier.

The author talks about the cyberattacks and the havoc caused by them in the digital world, with impact on the physical environment. The growing dependency on computer systems has made them vulnerable and attractive targets for an attack by both state and non-state actors. According to Latiff, the US Cyber Command and NSA have successfully foiled many cyber-attacks on US critical infrastructures, though he does not highlight specific incidents as examples. He, however, cites many examples from history of wars—from Julius Caesar's campaign to Rome in 49 BC, wars in the 17^{th} and 18^{th} centuries, WWI, WWII, the 2003 invasion of Iraq. The author explains how the introduction of new weapons and their advancements has changed the course of combat tactics.

At present, US is not only threatened by the Islamic State (IS), the al-Qaeda and the Taliban, but also its old rivals—Russia and China that compete with the US in technology and modern weapon systems. The author displays a deep sense of fear and emphasises that the US must accelerate its development programmes of new technologies and weapon systems in order to counter the growing threats.

This book will of great interest to anyone who is following the integration of advanced technologies and weapon systems. It helps us better understand the changing aspects of the advanced military technologies and also their adverse consequence for human society. The book is a wake-up call to those who still believe that nation's victory in a battle or war would continue to depend largely on more familiar conventional weapons and platforms rather than 'future technology-enabled' weapon systems.