Review of John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare*, Polity, 2021; Nicole Perlroth, *This is How They Tell Me The World Ends: The Cyber Weapons Arms Race*, Bloomsbury Publishing, 2021; and Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press, 2020

Cherian Samuel*

John Arquilla could be said to be for cyberwarfare what Vint Cerf is for the internet. Widely credited with coining the term 'cyberwarfare' more than two decades ago, Arquilla, a professor of defense analysis at the U.S. Naval Postgraduate School in Monterey, California, has been a veritable fly on the wall at many crucial points in the US development of its strategies for cyberspace. This, as well as his background as a defence analyst, makes him uniquely positioned to give a historical perspective on many of the issues related to cyberwarfare, and explain why militaries, even one as technologically advanced as the US military, have been so slow in adapting to cyberspace.

Bitskrieg: The New Challenge of Cyberwarfare sets out to give an overview of cyberwarfare, its various manifestations in peacetime through cyberattacks, what it portends for warfare in general, as the

* Dr Cherian Samuel is Research Fellow at Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi.

ISSN 0976-1004 print

Journal of Defence Studies, Vol. 16, No. 2, April–June 2022, pp. 101–110

technologies mature, and how best to tame the unbridled use of these technologies through arms control measures.

The book is divided into five chapters; the first chapter titled 'Cold War Rising' looks at the evolution of cyber war, the next chapter 'Pathways to Peril' deals with different forms of cyber war as well as cyber terrorism and attacks on critical infrastructure. The third chapter 'Next Face of Battle' deals with the subject of the book's title, *Bitskrieg*, which is a take-off on the German strategy of *Blitzkrieg* employed with devastating effect to annihilate opposing forces. Just as *Blitzkrieg* employed advancements in technologies to improve the balance in favour of the attackers, *Bitskrieg* seeks to use new technologies from drones to artificial intelligence to engineer new concepts of warfighting such as swarming. Arquilla goes into the historical records to show that new technologies start with a wild west phase as the envelope is pushed to the extent possible, at the cost of much destruction and loss of human lives, followed by a phase where the worst excesses of the new technologies are aimed to be curbed through mutually negotiated Arms Control agreements. This forms the subject of the fourth chapter, 'Arms (Ctrl+Alt+Esc)'. As in the previous chapter, past is taken as prologue, and earlier attempts at arms control and the extent to which they succeeded and failed, and the reasons thereof, are examined in this chapter. He accepts that the unique characteristics of cyberspace and cyber technologies make it less than certain that arms control measures will succeed, but adds that, nevertheless, attempts have to be made since the alternative would be absolute chaos. He sees greater possibilities of success for behaviour-based arms control as has been successfully carried out through the Chemical and Biological Weapons Convention. The last chapter, 'Through a Screen Darkly', highlights the points made in the previous chapters and also speaks in broader terms about the need for new mindsets in order to take cyberspace to a new era, one in which countries are mature enough to come out with rules of the road and restrain themselves from attacking critical infrastructure and content to use cyber weapons strategically rather than to just spread chaos.

Within this broader framework, Arquilla also tries to frame answers to many of the conundrums surrounding the US approach to cyberwarfare, which is yet to hit its stride, despite its first mover advantage. Arquilla begins by quoting Martin Libicki, who described cyber conflict as a 'mosaic of forms' ranging across the various modes of military operations and having significant psychological, social, political, and economic

aspects as well. Through much of the book, he delves into each of these aspects to draw out how they have in turn influenced the evolution of cyberspace. The US has had an outsized impact on its evolution since it is predominantly an American invention, if it can be called that. The blame for the lack of security controls, which has proved to be a major lacuna, can be laid at the door of the market-driven economic structure of the American society where consumers have privileged cost and convenience over security. This has led to market failure to address an important issue as well as the ensuing path dependence which has made it difficult to go back and incorporate security since it has become a *fait accompli*. He further notes that while market failure is usually compensated by regulation, privacy concerns have come in the way of the government establishing and sustaining regulatory roles in cyberspace. Regulatory and market failure is also seen in the condoning of the cyber security business sector continuing to flog inadequate tools such as antiviruses and firewalls since they have invested heavily in the development of these tools.

Besides such broader insights, the main focus of this book is on the complete reboot required by the military, both in terms of doctrinal thinking and organisation, to leverage these technological advances for warfighting. As he puts it, advanced information technology has profound implications for military organisations, doctrine, and strategy. Most militaries have simply grafted on new information technology tools to existing practices; the mindsets are yet to change in step with the technology. Path dependency can be seen leaching into even military alliances like NATO where the American penchant for preferring offense over defence in cyberspace has shaped NATO military thinking leaving the less capable countries in the alliance vulnerable to cyberattacks. As he puts it, American influence on the way in which cyber ought to be understood has kept 'NATO from developing a holistic view of how advanced information technologies can be interwoven into overall military affairs'.

Arquilla delves into history to show that there is a pattern to how technological advances get incorporated into the military and lead to changes in military thinking. However, the period between the development of a new technology and the road leading to its eventual adoption and maturity is a long one fraught with all kinds of unpredictable consequences. As Leon Panetta, former US Secretary of Defence pithily puts it in his foreword, "in the history of warfare the initial periods

when new weapons were developed were often the most dangerous. The possessors of the new technology saw themselves as having a unique advantage but one that was fleeting creating a use it or lose it mentality. It was also the period when the technology and its consequences were least understood. The result was devastation unequalled for the time."

The crux of Arquilla's argument is that military transformations are not simply technological; to earn the moniker of a revolutionary change in military affairs, the new technologies and the tools coming out of these technologies must result in a change in military organisation and a change in doctrine. However, such re-organisation is anathema to big organisations, and militaries are the biggest of them all.

Arquilla devotes the next chapter to examining those technologies that are most relevant for the military, including robotics, and artificial intelligence and the possible uses of attacks such as swarming from which he derives the name of his book *Bitskrieg,* which is an alliteration of the *Blitzkrieg* technique used by the Germans in World War II taking advantage of the then technological innovations such as air power, and mechanised quick moving infantry undertaking surprise attacks.

Another chapter is devoted to the issue of cyber arms control, whether it is doable and what shape it could take. Here again, he goes back into the history of cyber diplomacy, and talks about a missed opportunity in the early days of cyberspace when the Russians were trying to get the Americans to agree to an arms control treaty. The idea of cyber arms control was unattractive to the Americans because they saw no reason to agree to anything that constrained their leadership position in this domain. This was a major short-sightedness according to him, since they did not realise that being ahead meant competitors would always try to catch up and an arms control treaty would at least have cemented the leadership position. Though traditional arms control based on monitoring is a non-starter in cyberspace, given its unique characteristics, his focus on arms control is not so much to control the weapons themselves but to control the use of these weapons or behaviour-based constraints. Arquilla suggests a behaviour-based ban on "the use of the virtual domain for purposes of engaging in covert economic and political warfare and to tamp down the urge to go beyond espionage by utilising intrusions for purposes of preparing the way for acts of strategic cyber-attack". He brings cyber theft of intellectual property as well as cyber sabotage within the ambit of cyber arms control as well as cyberspace based political warfare like misinformation, the ultimate aim of these measures being to limit

the attacks on civilian infrastructure both in peace and war times. The only dimensions to be excluded are the use of artificial intelligence for military purposes and integration of robots into warfare, chiefly because that is where he sees the future of warfare.

According to him, the most significant gains in military effectiveness are going to come from a skilful blending of humans and intelligent machines in combat formations which can employ battle doctrines such as swarming. He goes as far as to say that artificial intelligence can take on the role of being a strategist since humans too easily suffer from information overload which prevents them from calculating outcomes based on the available information with high reliability. Machine learning may provide planners and decision makers with fresh insights.

While there are umpteen books on the subject of cyberwarfare and cybersecurity, this book stands apart by virtue of the fact that the author has been amongst the most long-standing observers of cyberspace and its development in all its dimensions. The book itself seems to have been long in the making, with its genesis in a 2011 article titled 'From Blitzkrieg to Bitskrieg: The Military Encounter with Computers', Communications of the ACM, October 2011, Vol. 54 No. 10, pp. 58–65. The book is written in a very comprehensible style, making it accessible to the general reader. Where it falters is in advocating a complete dependence on the new and evolving technologies, even as the author himself acknowledges that there are still many vulnerabilities to be secured, with the "goal of having truly secure information systems remain[ing] tantalisingly within reach but just beyond most military's grasp". So even if "in an earlier era your power was measured in terms of information you could control; and now and in the future, your strength will be measured by the amount of information you share", this depends on securing the networks first. Worth mentioning are anecdotal insights and interesting analogies such as this one; the notion of cyberspace being like a frontier zone in the physical world has its limits. "Real frontiers", whatever their size, tend to be reduced as they are settled, cultivated, ultimately tamed. But cyberspace is a wilderness that continues to grow, faster than the rate of "settlement" of some of its areas. Expansion of the virtual domain creates many fresh ungoverned spaces affording new jumping-off points for those who would "raid already settled areas to steal their intellectual property, kidnap data, and hold it for ransom, engage in other forms of commercial extortion, and perhaps even try, via political warfare, to upset the basic processes of governance".

This book's approachable style of writing makes it useful reading both for specialists as well as the general public. The latter would find it more useful to read this in conjunction with one of the books mentioned by Arquilla in his list of further readings. *This is How They Tell Me The World Ends: The Cyber Weapons Arms Race*, published in 2021, is a deeply engaging book by Nicole Perlroth, a cybersecurity reporter with *The New York Times* who has written many cyber-related stories. This book expands on the many incidents mentioned by Arquilla in his book and provides the backstory combining both reportage and analysis, thus filling many of the gaps in understanding for the general reader, as well as further comprehension of some of the more radical ideas propounded by Arquilla.

The book consists of 23 chapters spread over eight sections. Whilst the first few chapters look at how zero-days (software vulnerabilities used by attackers to penetrate computer systems) are the fuel for the cyber weapons arms race since they are the point of entry for most cyber weapons, subsequent chapters look at the roles played by various individuals, companies, and governments to keep the arms race alive with a similar cohort working to tamp down these efforts.

The story begins with bug bounty programmes, which were instituted to incentivise programmers to locate bugs in software and inform companies for a price. This led to government agencies also buying up these bugs but with the less than honourable intent of weaponising these bugs and utilising them for breaching computers and networks of countries of interest. The natural progression then as detailed in the section titled 'The Spies' was for government agencies themselves to build up expertise in-house to locate these bugs rather than depend on hackers. The success of Stuxnet, which was a joint US–Israel cyber operation against Iran and cyber-attacks from Russia in the first decade of the 21st century, meant that the focus turned to retaliatory attacks rather than building up better defences, according to Perlroth. From 2009 till 2012, the NSA's (National Security Agency) budget tripled from US$ 2.7 billion to US$ 7 billion. Another US$ 7 billion was also budgeted for cyber activities across the Pentagon resulting in a total budget of US$ 14 billion. Recruitment also skyrocketed with 900 dedicated personnel to 4,000 and eventually 14,000 by 2020. Then President Obama also ordered the intelligence community to produce a list of cyber targets, including infrastructure, processes, and systems and "preparing the battlefield". According to Perlroth, this policy response was incredibly

short-sighted since the US was itself most vulnerable to cyber-attacks. At every inflection point, the US inevitably chose the wrong path out of the many available.

Even as the zero-day market was maturing in the US, it was also expanding abroad with intelligence agencies from many countries also buying up zero days at a frantic rate. Companies around the world were now offering hacking services to governments as "guns for hire". All of these developments led to what she describes as the perfect storm, countries hacking other countries and companies, non-state actors employed by states for plausible deniability carrying out tasks assigned to them by day and engaging in cybercrime after office hours, large-scale data breaches which were then sold to the highest bidder or leaked to cause the maximum damage to companies and governments. Many of the attacks are laid out in great detail in sections looking at attacks from the main actors—China, Russia and Iran—with the underlying reasons and approaches. Perlroth's conclusion after this detailed examination of the origins of these cyber skirmishes, and their expansion into full-scale cyberattacks, is that the US missed several opportunities to take the lead in securing the stability of cyberspace. In some instances, as with the Stuxnet attack, it fired the first shot, leading to the subsequent attacks on its infrastructure. With Russia, it refused to discuss cyber arms control, though whether such measures were feasible or sustainable was another issue. With China, the Obama–Xi summit of 2015 saw a reduction in cyberattacks, but a change of government in the US and President Trump's more aggressive approach towards China put a premature end to that agreement. The present situation is that the chickens have come home to roost with the US remaining as vulnerable as it was a decade ago, while hostile actors continue to carry out successful attacks against virtually every part of the government, economy and society with impunity. These attacks have become more sophisticated and destructive over the years, and it is evident that all sides have even more sophisticated cyber weapons that they are holding back for strategic reasons. The irony is that many of the weapons being used against the US were developed by the US NSA and were obtained by hostile actors after the agency was hacked, even though the NSA continues to deny that this was the case. With software containing as many vulnerabilities as there are stars in the sky, "this state of insecurity and instability in cyberspace looks set to continue indefinitely".

While the title of the book gives the impression that this covers cybersecurity issues in other countries, the main focus is on the US. Perlroth looks at other countries only to the extent of their attacks on the US. Nonetheless, the lessons of the book applies equally to all since attacks can be targeted against any country of interest in the borderless and globalised world of cyberspace where the same software with the same vulnerabilities can be used across countries, corporations and by the common man as well. Whilst Perlroth's book lays out the extent of the problem very starkly and shows how it will not go away unless underlying problems are attended to, and there is an attempt by countries to negotiate in good faith to bring back a semblance of stability and security in cyberspace, Arquilla's book lays out the alternative which seems more and more an inevitable reality; a bleaker world where newer and more advanced forms of technology only leads to less, not more, security. Not having learnt any lessons from the past, new technologies are seized on as the panacea for old sins. Even though the possibilities of arms control are dealt with at length in his book, it is doubtful whether similar discussion is taking place in the chambers of the policy-makers around the world, given the impression that there is much more left to be exploited with cyberspace.

The definitive volume that ties all the threads together to present the past, present and future of malicious cyber activity is Ben Buchanan's *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Buchanan traces the origins and changing role of malicious cyber activity within geo-politics of over the decades, and where it is placed today. The 13 chapters of the book are divided in three parts, titled 'Espionage', 'Attacks' and 'Destabilisation' which are, respectively, the main goals behind most malicious activities in cyberspace today. As with the other authors, he notes that the US exploited its "home-field advantage" by not using its technological prowess and pole position to further cyber-security. Instead, it went proactively in the other direction by hacking into the networks of friends and foes alike for espionage purposes. This could only be considered as perfidy, were it not for the fact that much of this was carried out by its intelligence agencies in active connivance with other intelligence agencies. The lure of information acquired through data collection was such that the US could use, for instance, its partnership with "Denmark's intelligence agency to spy on Germany and a similar partnership with the German intelligence agencies to spy on Denmark." Even the proliferation of such capabilities proved beneficial

for US intelligence agencies as they provided opportunities for "third" and "fourth" party collection. An example of the latter was the "US agencies spying on South Koreans who were spying on the North Koreans spying on other countries." The emphasis on espionage and offensive capabilities for the US was underlined by the dictum of "nobus", i.e., *nobody but us*, when it came to the most advanced capabilities.

Countries hostile to the US at the receiving end have responded by developing their own capabilities and using them to attack American critical infrastructure and networks. The titles in the chapters in the section titled 'Attack', namely, 'Strategic Sabotage', 'Targeted Disruption', 'Coercion' and 'Testing and Demonstration' speak for themselves as to the goals of these attacks. If the ultimate goal is strategic deterrence, he notes that very few countries have been successful at this because elements such as signalling are very difficult to achieve through cyber operations.

The last section on destabilisation covers not just societal and political destabilisation attempts as in the electoral interference attempts in the US, France and elsewhere, but also attempts at destabilising the intelligence agencies also through the tit-for-tat exposures of the tools used by intelligence agencies to carry out their malicious activities in cyberspace, nevermind the consequences. The "sabotage for exposure" of the US NSA's "Eternal Blue" set of exploits was subsequently used in the *WannaCry* and *NotPetya* attacks which led to staggering losses (estimated at around US$ 14 billion) for businesses around the world.

The inferences that can be drawn from this book are that signalling is very difficult to achieve through cyber operations, given its unique characteristics, complexity and ease of misrepresentation. Secondly, for pretty much the same reasons, the attempts at framing rules of the road for cyberspace will be a long and arduous process, mainly because the malicious actors will always be one step ahead and major cyber powers are more interested in developing offensive capabilities rather than shoring up their defences through, amongst other measures, the implementation of norms and conventions. The misuse of private enterprises for the purpose of intelligence collection has increased distrust and will lead to the fragmentation of cyberspace as erecting of data barriers and calls for indigenous development of technologies that are an inevitable outcome, leading to trade, industrial and technology restrictions.

Despite the complexity of the domain, the author has crafted a very readable exposition, with each section of the book replete with detailed

case studies of well-known cyber-attacks, often bringing up hitherto unknown aspects of these attacks. The antecedents of WannaCry, as a case in point, are traced in great detail, including all the different conjectures about who was behind the hacking of the Tailored Access Operations (TAO) group from the NSA, how it could have been carried out, to why it was released into the wild, ultimately leading to the WannaCry ransomware attack. Of particular interest to Indian readers will be the detailing of the hacking of the Pune-based Cosmos Cooperative Bank in 2018 by presumed North Korean hackers. This successful hack was made at the backdrop of many unsuccessful attempts on banks in other parts of the world which failed at the last stage when the money was to be withdrawn. In this particular instance, money mules in 28 countries used cloned ATM cards to withdraw about US$ 11 million. This, they were able to do, by apparently taking over the authentication servers as well. In this regard, Buchanan's book is in line with his earlier work, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Hurst, 2016), which also had detailed case studies to illustrate his arguments on the subject.

Individually, and collectively, these books are an eye-opener to the changing nature of conflict in cyberspace. The fact of the matter is that while countries are publicly professing the goal of a stable cyberspace, there is frenetic activity going on behind-the-scenes to ramp up offensive capabilities, as cyberspace becomes a fulcrum of global geo-political competition. The sooner we face up to this truth, and adjust our policies accordingly, the better it would be.