A Review of: "Bitskrieg: The New Challenge of Cyberwarfare" by John Arquilla[1]

Attila Gulyás[2]

For the new aspects of cyber and traditional warfare, one can hardly find a more credible expert than John Arquilla, who is one of the leading national security thinkers of our time, and whose career and expertise are a guarantee for valuable analysis for both cyber experts and the general audience[3]. In this book the author reveals the challenges of the cyber security of our era and connections between cyberwarfare and traditional warfare, which result in a new type of warfare.

Not long before the Second World War the Germans created a new form of warfare which is based on the artistic combination of tanks- planes- and radio communication. This was called "Blitzkrieg" and in the wake of the war it helped the Nazis subjugate a part of Europe. Fortunately, the allies learned from the lesson and in a short period of time they built the new methods in their military strategy. These methods are present even today in the military way of thinking.

But the world has changed dramatically, especially in the last few decades. Due to new inventions and the revolution in information technology a new domain has been born, which is called "cyber world", where new players demand roles. Countries like Russia, China or the Democratic People's Republic of Korea (DPRK, also known as North Korea) developed new cyber capabilities which can be used to undermine the faith in the accuracy of the voting process, steal the cutting-edge intellectual property of international firms, or support their country by stealing fiat and crypto currency in addition to the proliferation of nuclear weapons. Even the earlier looked-down, third world African countries like Zimbabwe or Sudan with the help of Iran and China are working on the improvement of their cyber capabilities. As for cybercrime, there is Nigeria where the "Yahoo boys" - the large-scale scammers - are playing their filthy games on behalf of "African princes" or sons of oil tycoons who want to

[1] Arquilla, John, Bitskrieg: The New Challenge of Cyberwarfare. Polity Press, Medford-Cambridge, 2021. ISBN-13: 978-1-5095-4362-5 (hc); ISBN-13: 978-1-5095-4363-2 (pb).

[2] Ret. LTC, researcher at Africa Research Institute, School on Safety and Security Sciences, Óbuda University, Budapest, Hungary; ORCID: 0000-0001-5645-144X.

[3] John Arquilla is an American analyst and academic of international relations. He worked for the RAND (American nonprofit global policy institute) for decades and he has been teaching courses in national security affairs and defense analysis at the NAVAL Postgraduate School. Arquilla worked as a consultant to General Norman Schwarzkopf during the Operation Desert Storm (1991), and the Kosovo War (1998-1999) he assisted United States Deputy Secretary of Defense on international information strategy. He also was one of the advisors to Secretary of Defense Donald Rumsfeld (2001-2006). Arquilla developed the concept of netwar, or "swarm-tactics" which is a particular fighting style of network organized groups. He is a promoter of the new idea of adapting the military structure to a network based model to be able to defeat terrorist networks.

evacuate their heritage from their cruel country or hunting for women to extort money from them.

Besides the State Actors there are many Non State Actors around such as terrorists, cybercrime organizations and different hacker groups - just to name a few - that are able to attack and paralyze critical infrastructure, steal money, etc. The new invention of our era is the IoTs (Internet of Things), the interconnected household appliances that can be organized into a multi millions zombie army, which can be weapon in the hands of hackers with malevolent intentions.

Today there is no balance between the offensive and the defensive capabilities. The attackers will keep their advances until the defenders can only rely on brick-wall like firewalls and anti-viral software solutions, because they are always a step behind advanced malicious software. It is obvious that the most important challenge is the improvement of security. The heavy encryption and the Cloudstorage where data is divided into pieces and distributed seem to be the only solution. Even the best remote cloud storage system is worth nothing if the encryption is weak because it lures the aggressors to attack our systems.

Apart from civilian society that can be the target of attackers in political and economic aspects the new warfare has military risks. New wars will be fast paced and the weapons and coordinated strikes of the swarms AI supported, where net and web-based communication is a vital component the interruption or slowdown of which by viruses or worms can lead to catastrophe in battle time. This kind of cyberwar that focuses on the “battle” is the successor of the Second World War “Blitzkrieg” which is called “Bitskrieg” by the author. The cyberwar will change warfare in many areas e.g. from the large formations to smaller, highly networked units which instead of mass on mass engagements to swarm battle tactics where the swarms and the members of the swarms are interconnected with heavily encrypted network based communications systems. The strategic goal is to know more than the enemy in other words to get the information edge. The basic concept is that an information edge is best exploited by “dislocating” enemy forces through the disruption of their communication, instead of confrontational direct or indirect flank assaults.

The consequences of political hacking or a cybercriminal act in the civilian sphere are negligible to the fatal effects of the military operations undermined by information insecurity. That is the reason why the armed-conflicts relations of cyberwar should be the subject of studies.

Unfortunately the varieties of the possible cyber threats are so wide that it is impossible to prepare for all of them. That is why, besides the improvement of cyber security and preparation for “Bitskrieg” like operations, there is one more challenge and it is arms control. But in this case the cold war nuclear bomb counting model based arms control does not work because the fruits of the advanced technology are multipurpose, which means they can be used either in civilian or military area. The idea of cyber weapon control at first seems meaningless, but as Arquilla argues it has a point. The behavior-based arms control has been

working for decades in case of biological and chemical weapons.

This kind of cyber arms control would provide the security of individuals, intellectual properties, and critical infrastructure in times of peace.

The above mentioned issues are only a part of topics discussed in details seasoned with colorful interesting historical examples taken from the military history of the world, ranging from ancient to present times. The author also introduces new expressions like “cool war”, or “Bitskrieg”, and interprets their meanings by putting them in context. The comparison of traditional war interpretation by Clausewitz is very interesting with the features of the new type of war as Arquilla refutes the principles that had ruled the military thinking for centuries. The author explores and presents the reasons for the vulnerability of the American cyber defense system with relentless sincerity, and at the same time, he gives possible remedies for this malady. Arquilla dedicates a chapter to cyber terrorism in which he logically explains why terrorists restricted their cyber activity to waging political warfare and propagandizing in ways that discomfit the enemy and aid in gaining popular support, and recruits, from among its target audiences. Not less intriguing is how Arquilla unveils the reasons and new - so far unknown - details of the failure of negotiations between the USA and Russia on cyber weapons control. In the light of recent events in Afghanistan, he emphasizes the mistakes of the military leadership in the war of Iraq and Afghanistan with undisguised honesty.

The author touched on many more exciting and thought-provoking topics in this book like the possible role of the AI in the military of the future on the battlefield and in strategic planning, not to mention the responsibility of the AI in decision-making.

The front cover image refers to the main thought of the book as the tank-mouse is the symbol where the tank is the representative of old-fashioned warfare while the mouse is the symbol of cyberwarfare that differentiates “Bitskrieg” from the “Blitzkrieg”.

The book is a must have for cyber experts and military thinkers who are interested in the actual issues of cyberwarfare and its effects on traditional warfare, and want to get a glimpse into the future, but even the general public may find it interesting and useful. My suggestion is to read the book more than once, as one can acquire new information and much more details by re-reading it.