Overcoming Complexity of (Cyber)War: The Logic of Useful Fiction in Cyber Exercises Scenarios

Marzio Di Feo

Abstract

The paper is an attempt to analyze the logic and the impact of "useful fiction" (or "fictional intelligence") in cyber exercises scenarios as an approach to prepare for future conflicts. Cyberspace increased the complexity of war phenomenon with its characteristics of artificiality, plasticity, and uncertainty. To overcome this complexity, cyber warriors need to adapt to everchanging scenarios. In this view, the development of a new epistemology of wargaming and cyber exercises could provide a deeper understanding of war and, thus, enhance the capability to cope with this instability. In this framework, fictional intelligence would enrich the research of (un)imaginable phenomena to prevent future threats.

Keywords

Cyber war, fictional intelligence, future of war, cyber exercises, wargaming

1. Introduction

'Would you have them train this way now?' Cosimo Rucellai asks in *The Art of War* (1521) to Fabrizio Colonna, Machiavelli's *alter ego*. Among the various exercise described, 'running wrestling, making them jump, making them work hard under arms heavier than the ordinary, making them draw the crossbow and the sling; to which I would add the light gun', swimming and horseback riding, on the latter, in particular, Machiavelli recounts, taking up Vegezio, how the 'ancients' practiced riding on a wooden horse, building imaginary scenes that could make such action 'easy' in real war. The use of simulation for military training has become a *de facto* standard in the face of the increased complexity of the war phenomenon and the uncertainty of future conflicts. At the same time, the growing militarization of cyberspace has placed nation states in a position to develop highly specialized cyber units as the first line of national cyber defense [1, 2, 3]. These units should maintain high capabilities of preparedness to ensure the readiness in hypothetical war scenarios through the support of training and simulations in cyberspace [4]. Indeed, the characteristics of cyberspace, such as the actor's ability to act in the shadows, as well as the plasticity of the domain, increase the uncertainty and undermine the attribution capacity[1] but, above all, affect the strategic implications of cyber attacks in terms of dynamics of conflict [5, 6].

In this context, the paper is an attempt to emphasize the logic of useful fiction for an epistemology of cyber exercises scenarios through the combination of two fundamental theoretical elements. The first concerns the theoretical understanding of war phenomenon as enhanced complexities by the intrinsic nature of cyberspace. The second, on the other hand, is based on the concept of fictional intelligence such as 'hybrid narrative of research and analysis' [7]. From a methodological point of view, the paper is presented in an openly speculative form on the theoretical perspectives and applications of the two concepts. Although, to strengthen the general hypothesis, we also recall some empirical evidence, however, the paper also aims to contribute to the broad debate around the changing human and machines

Proceedings Name, Month XX–XX, YYYY, City, Country
EMAIL: marzio.mdf@gmail.com
ORCID: 0000-0003-4167-5058

[1] There is a large literature on the attribution problem, which will not be the subject of this paper. For an overview of the debate see, *inter alia*: T. Rid, B. Buchanan, Attributing Cyber Attacks, Journal of Strategic Studies 38 (2014) 4-37.

relations in war arguing that fictional intelligence and creativity help the understanding of the imaginary around future threats while exploring the consequences of the cyberspace environment on the war phenomenon.

2. Cyberspace and the changing character of warfare

Modern conflict scenarios push battlefield out of materiality and its geographical frontiers. Cyberspace is a "placelessness" environment *par excellence* due to its intrinsic characteristics of volatility and plasticity as artificial or man-made domain [8]. Moreover, humans have to be prepared to cope with unpredictability of complex operations theatre and to redefine the relation with machines, on which more and more rely on.

Today's wars are being fought in data-rich environments, where large amounts of information and data come from every device on the ground. As a consequence, fusing with the machines, soldiers need to improve their own individual fitness in particularly stressful and uncertain situations. This shift seems to be in turn validated by the dependence on cyberspace, and the need for a cyber warrior to adapt with an everchanging scenario [9]. Data flow or the reliability and the availability to increase performance and battle situational awareness, posing a cognitive challenge to humans coordinated in understating and adapting to fight at the dependencies of and (no-)filtered information. This *brain* where data fusion is centralized disseminates data from cyber systems, drones, satellites, vehicles, and soldiers on the battlefield, from all the sensor producers to those entities configuring an interconnected system. And *dataism* [10] comes to the war: more and more devices are connected to each other with the need to be *secured*. If we could imagine an acting metamorphosis that could transform cyber warriors in software and hardware components to jump off into the cyberspace, they will discover a virtual contested space that in many ways offers access to information and opposing forces which seek to curtail that access. Underlying Arquilla and Ronfeldt [11] distinction between "netwar" and "cyber war" and, as Singer [12] shows, contested data is now everywhere. This debate on cyber war and, in general, on war and technology in International Relations has been very fruitful and has brought some useful conclusions [8, 9, 13]. In this view, we draw on the possibility of understanding some dynamics of the evolution of the war phenomenon through the lenses of Clausewitz, considering some of the limits of the discipline to fully understand the implications of cyberspace environment with particular reference to the relationship between human and machines for the understanding of war. From this point of view, we are interested in analyzing war as an object *per se* [14] and not the social constructions that derive from it.

On the other side, in the military field, the digitalization of battlefield also imposed to enter into the algorithmic logic of information [9, 15]. Algorithms are complex codes that largely determine how information is flowing and that decides what kind of information has to appear on the screen. This changing nature of war due to technological progress in the cyberspace environment also involves the increased presence of robotics, drones, and remote guided weapons on the ground [12]. Moreover, this reveals the power of virtuality as 'ability to collapse distance, between here and there, near and far, fact and fiction' [16, p. 776]. The large amount of data, encompassing all the physical domain, as a hypermedia loop, also impacts military strategy in the cyber domain [17]. In future warfare, flexible and complex dynamics have to be managed by human-machine teams, placing serious issues on the ability of the first to maintain agency on the second [15, 18]. Thus, however, the performance of this interaction will have sweeping social impacts, changing many aspects of how we live, learn, communicate, and fight.

3. Clausewitizian *ratio* against the complexity of (cyber)war

The 'logical' life of information systems was to put 'order' in warfare as a way to cope with chaos, attrition and 'fog of war' for a synthesis that enables domination of the battlefield as fragmented disorder of reality. Information age technology has changed the nature of warriors, forcing the need of continuous information and feedback [19]. Complexity emerges from the interactions of interrelated elements and the study of such emergent behavior needs to understand how the attempt at dominating uncertainty involves the fusion between humans and machines. Information plays a decisive role as its

use is fundamental for the management, planning and conduct of operations in contested domains and in a condition of continuous conflict. The greater the quantity of information, the greater the possibility of misperceptions, of noise and error. Moreover, the tensions between conventional and non-conventional actors and different ways of conducting war, irregular and cyber, entails the idea of a complex and interconnected battlefield, where the enemy disappears to use the words of Zohar [20].

War does not jump, but it adapts to technological changes. Information and systems integration, and the greater future autonomy of these systems, are part of these changes. The wide dissemination of information, the data collected from almost every social interaction or shift in logistics, were up to a few years unimaginable in the context of war confrontation [15].

Man produces data, the machine collects them, and man, for now, reinterprets them [21]. At the same time, critical infrastructures are the epitome of the nervous system of a state, and it is no coincidence that some developments in the literature have seen in defense and cyber attacks on critical infrastructures the evolution of strategic thinking about strategic bombing [22]. In this perspective, the protection of critical infrastructures represented the ecosystem of war confrontation in cyberspace.

In addition, sophisticated modeling through the use of predictive tools in real time allows constant self-awareness, obtaining a continuous return on the effectiveness of the actions. For example, analyzing and creating suitable models according to the dynamics concerning the specific target can increase decision-making skills up to an attempt to predict the behavior of subsystems or systems within the context [23]. These perspectives of complexity can be seen in the resumption of some elements of the chaos of war as such and exasperated by the cyberspace which has a multiplier effect. Keeping in mind the Clausewitzian view in Rid [24] for which 'cyber war will not take place', here we try to investigate, as mentioned above, the characteristics of the war phenomenon and not the consequences of it. This attempt allows, in fact, to draw the relationship between the three causes of uncertainty, following the perspective outlined by Beyerchen [25] and the non-linearity of the war phenomenon in a non-linear context. (1) War is a duel (*Zweikampf*), a clash of opposing wills, which aims to bend the opponent: this interaction is the fundamental cause of uncertainty, its dialectic, its irrationality, exponentially increased in hyper-connectivity in unpredictable environments since subject to man [26]. (2) War itself is an unstable system by nature. The second element of unpredictability is friction, or Clausewitz's Murphy's law, factors not necessarily present in the conflict but, nevertheless, to be considered as endogenous variables, decisive for giving a negative turn to circumstances and compromising its outcomes [27]. A noise in the information process thickens the fog of war (*Nebels des Krieges*), its opacity, making the clash of wills like physical entropy: a loss of energy in action against a resistant medium [25]. The human difficulty consists precisely in managing an enormous mass of information in a correct and suitable way to make a type of decision. (3) War is the sphere of chance, the third factor of instability. This is strongly influenced by the high number of elements in the war phenomenon with the same dynamics of a game of cards [25]. Chance is the cause of the analytical blindness of those who have to make decisions, when a sudden change in the initial conditions brings out ill-considered nuances. In this sense, the Clausewitzian *ratio* of war can be understood as the entropy of the phenomenon due to the human interactions present in it [28]. Simulated scenarios are shaped by a new human-machine relationship [29] and, at the same time, they represent the tool to prepare for this complexity.

4. Epistemology and practices of wargaming and cyber exercises

Computer simulation, both from the point of view of political decision-making and for intelligence activities, or for the military operations and training, have a role of primary importance in understanding and preparing for the unpredictability of complex environments [30, 31]. Faced with this evolution, the ability of wargaming has been seen as a tool for dynamic representation of conflict in a synthetic environment, in which actors make decisions and respond to the consequences of those decisions: from abstract to simulation, and from simulation to story based on experiences and studies [32, 33]. In this perspective, wargaming can be understood as a scientific method of providing decision makers with a quantitative basis for decisions. In national strategies, the belief was increasingly advanced that for thinking the unthinkable the simulation of what-if scenarios could contribute in terms of understanding

the subsequent strategic and political dynamics [34]. Then, the application of wargaming combined technological developments with the difficulties of determining threats[35].

At a strategic level, the implications of cyber attacks have been addressed and developed in several exercises in the context of simulated cyber defense scenarios in the face of large-scale attacks involving all aspects of the decision-making process and chain of command (e.g., NATO cyber exercises Crossed Swords and Locked Shields) [36, 37]. Factors such as anonymity and the ability to operate in the shadows act as multipliers of the complexity of the evolution of the exercises scenarios. Thanks to its plasticity, the cyber domain also offers the possibility of deceiving the opposing actor through deception activities. In fact, the empirical evidence relating to the possibility of deception, in this context, is numerous as reported by several scholars and analysts [38]. Indeed, if, on the one hand, the ability to attribute an attack requires an accurate analysis of information, on the other hand, attribution is not free from political and strategic implications by intervening on the possibilities for political and military escalation. The sophistication of the attack, then, decreases the chances of correct attribution if, for example, it is carried out by non-state actors financed or supported by highly structured actors such as APT (Advanced Persistent Threat) [39]. From the point of view of the simulated exercise, considering the strategic and political implications, in a given scenario, cyber attacks allow testing the possibilities to understand the complex interactions for future threats, while the speed of reaction increases the possibility of mitigating the effects and the consequences in the short and long term.

5. Imagining the future of cyber conflict through useful fiction

The concept of useful fiction, or fictional intelligence (FICINT), can be seen as a 'hybrid of narrative and research analysis' [7] and is used by actors to build the appropriate narrative on upcoming products and services.[2] The influence of fiction on the real world and, in particular, in the search for new ways of making and waging war is not new, indeed the fictional aspect has often been used as an inspiration for soldiers and decision makers [15], from Homer's Iliad to the books of Philip K. Dick or John Le Carré. FICINT combines, in a certain sense, the ability to envision age and communication by uniting writers and graphic novelists with a rigorous and scientific process and analysis. The recent attempt by the French Army to recruit a 'red team' of sci-fi writers to predict future threats represents a way to innovate and think about (un)imaginable disruptive scenarios [40]. The strength of this type of conceptualization therefore lies not so much in the predictive or explanatory capacity of a given phenomenon, but in the possibility of preventing future issues and threats. An example of useful fiction is represented by crowdsourcing from various disciplines to combine different approaches and, at the same time, be a hotbed for new talent [41].

As Cole and Singer [7] show, the usefulness of FICINT lies in some key elements. The first is, therefore, the ability to 'feel' the effects of the state of research through imagined worlds that favor empathy and critical thinking, perceiving, for example, the future of land warfare through the story of a soldier on the ground [7]. The ability of FICINT is to create and induce the user's emotional connection with a specific situation or problem. In this vein, the incipit of the US Cybersecurity Solarium Commission [42], written by Singer and Cole, is a short story of a 'warning from tomorrow' that imagines the disastrous consequences of a cyber attack, trying in a persuasive way to make the reader understand the starting point of new policy choices: 'The rainbow of colors in the window paints how everything went so wrong, so fast. The water in the Potomac still has that red tint from when the treatment plants upstream were hacked, their automated systems tricked into flushing out the wrong mix of chemicals (…). All around the Mall you can see the black smudges of the delivery drones and air taxis that were remotely hijacked to crash into crowds of innocents like fiery meteors' [42, p. ii].

The impact of the FICINT could therefore be evaluated in the possibility of being adherent to reality, i.e., to reflect problems and points of view that must contain, to take up what has been said above, even the fog of the war: the potential of this type of exercise lies precisely in this ability. It follows that in the perspective outlined here of cyber exercises scenarios, FICINT could highlight the technological

[2] Some practical examples include Ford's City of Tomorrow, and the graphic novel Two Days After Tuesday developed by the U.S. Army Cyber Institute, Citibank, the New York Police Department, and Cisco's Hyperinnovation Living Labs. See B. Merchant, Welcome to the Sci Fi Industrial Complex: Nike and Boeing Are Paying Sci-Fi Writers to Predict Their Futures, OneZero, November 28, 2018.

potential already in place with extreme scientific and analytical rigor, reflecting the dynamics of the real world [7].

The combination of cyber exercise scenarios and FICINT provides the possibility of increasing the ability to perceive change together with the possibility of debunking the veil of common sense by nurturing the ability to adapt to what-if scenarios. The strength of this type of mixed approach could derive paradoxically from the limits of scientific validity, i.e., use past data to predict future physical events, or no real war means data comes from models, and by the difficulty of internal validity, i.e., measures and instruments, as well as on repeatability [32]. This approach is aimed at defining a new epistemology based on the awareness to reshape the conception of the world and feed a powerful experience to research of critical phenomena, while the wargame [32, 34] becomes the tool to develop new hypotheses in a continuous cycle of exercise, analysis, and experience.

6. Conclusions

Approaching the theme of war and cyberspace requires a redefinition of the methodological framework. Its specificity provides a new theoretical language adapting classical elements of war and politics to 'doomsday machine age' [43]. Deterministic models could appear too simplistic tools to process complicated inputs by considering hypothesized mechanism, and then generate their consequences as prediction. As opposite, the complexities of cyberspace require the understanding of these dynamics as an adaptive system: a machine copying with changing circumstances [44]. Studying human and machine integration in the dynamics of conflict needs experimentation based upon tools for cyber knowledge. Perspective on science and nature in terms of systems, structures, and models is not an *in vitro* manipulation of key variables; and preparing for future war is not like an exercise on a wooden horse.

From another angle, a simulation approach, subverting Cartesian dualism, helps to get along in a world that can always surprise far away from deterministic trend, interpreting human actions the acting machine within the information environment. Thus, also cognitive process in artificial intelligence (AI) and performative interpretation of human actions pose a methodological question if theory itself (and systematic comprehension of reality) could arise from the adaptation in transforming world in an ontological shift from cyber tools as object to cyber tools as projects: a re-structuration of knowledge through new representational form of cyber exercise scenarios. Simulation in this perspective starts with a set of specific assumptions and rules rather than direct measurement of the real world (unlike induction), but it does not prove theorems (unlike deduction): cyber exercises can be interpreted as an aid intuition, the only viable way to study actors (i.e., humans and machines) who are adaptive rather than fully rational. Its value does not aim to provide a highly complicated representation of the real world but to enrich our understanding of a fundamental process that may appear from the capabilities to respond to future threats.

7. References

[1] R. Bendrath, J. Eriksson, G. Giacomello, From 'Cyberterrorism' to 'Cyberwar', Back and Forth, in: J. Eriksson, G. Giacomello (Eds.), International Relations and Security in the Digital Age, Routledge, Abingdon, 2007, pp. 57-62.

[2] R.C. Maness, B. Valeriano. Cyber War Versus Cyber Realities: Cyber Conflict in the International System, Oxford University Press, New York, 2015.

[3] B. Buchanan, The Hacker and the State Cyber Attacks and the New Normal of Geopolitics, Harvard University Press, Harvard, 2020.

[4] J.J. Li, L. Daugherty, Training Cyber Warriors. What can be learned from Defense Language Training?, Rand Corporation, Santa Monica, 2015.

[5] E. Gartzke, The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, International Security 38 (2013) 41-73.

[6] B. Jensen, B. Valeriano, What do we know about cyber escalation? Observations from simulations and surveys, Atlantic Council, 2019. URL: https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf.
[7] A. Cole, P.W. Singer, Thinking the Unthinkable with Useful Fiction, Journal of Future Conflict 2 (2020).
[8] C. Gray, The Future of Strategy, Polity Press, Cambridge, 2015.
[9] C. Coker, Warrior Geeks. How 21st Century Technology is Changing the Way We Fight and Think About War, Columbia University Press, New York, 2013.
[10] Y.N. Harari, Homo Deus. A brief History of Tomorrow, Harvill Secker, London, 2016.
[11] J. Arquilla, J., D. Ronfeldt, Cyberwar is Coming!, Comparative Strategy 12 (1992) 141-165.
[12] P.W. Singer, Wired War. The Robotics Revolution and Conflict in the 21st Century, Penguin Press, London, 2009.
[13] H. Langø, Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security, Working Paper 820, The Norwegian Institute for International Affairs (NUPI), Oslo, 2013.
[14] A. Bousquet, J. Grove, N. Shah, Becoming war: Towards a martial empiricism, Security Dialogue 51(2020) 99-118.
[15] L. Freedman, The Future of War. A History, PublicAffairs, New York, 2017.
[16] J. Der Derian, Virtuous War/Virtual Theory, International Affairs 76 (2000) 771-788.
[17] L. Ablon, et al. Operationalizing Cyberspace as Military Domain, Perspective, Rand Corporation, Santa Monica, 2019. URL: https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf.
[18] C. Coker, Still 'the human thing'? Technology, human agency and the future of war, International Relations 32 (2018) 23-38.
[19] D.S. Alberts, et al., Understanding Information Age Warfare, CCRP (Command and Control and Cyber Research Portal), Washington DC, 2001.
[20] E. Zohar, Israeli military intelligence's understanding of the security environment in light of the Arab Awakening, Defence Studies 15 (2015) 203-234.
[21] J. Shaw, Why 'Big Data' is a big deal. Information science promises to change the world, Harvard Magazine, March 2014. URL: http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal.
[22] S.J. Collier, A. Lakoff, The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem, in: M. Dunn Cavelty, K. S. Christensen (Eds.). Securing 'the homeland': critical infrastructure, risk and (in)security, Routledge, London and New York, 2008, pp. 17-39.
[23] K. Cukier, V. Mayer-Schönberger, The Dictatorship of Data. Robert McNamara epitomizes the hyper-rational executive led astray by numbers, MIT Technology Review, May 31, 2013. URL: https://www.technologyreview.com/s/514591/the-dictatorship-of-data/.
[24] T. Rid, Cyber War Will Not Take Place, Journal of Strategic Studies 35 (2012) 5-32.
[25] A.D. Beyerchen, Clausewitz, Nonlinearity and the Unpredictable of War, International Security 17 (1992) 59-90.
[26] C. Clausewitz, M. Howard, P. Paret, B. Brodie, On war, Princeton University Press, Princeton 1984 [1832].
[27] Visco, E.P. (2012). Murphy's Law is Alive and Well: Clausewitzian Friction on the Modern Battlefield. 29th IS-MOR Symposium. Retrieved March 12, 2021, from http://ismor.cds.cranfield.ac.uk/29th-sympo-sium-2012/murphys-law-is-alive-and-well clausewitzian-friction-on-the-modern-battle-field/@@download/paper/29ismor_visco.pdf.
[28] A. Bousquet, The Scientific Way of Warfare. Order and Chaos on the Battlefields of Modernity, Columbia University Press, New York, 2009.
[29] Y.H. Wong, et al., Next-Generation Wargaming for the U.S. Marine Corps, Rand Corporation, Santa Monica, 2019
[30] R. Axelrod, Advancing the Art of Simulation in the Social Sciences, in: J.P. Rennard (Ed.), Handbook of Research on Nature Inspired Computing for Economy and Management, Idra Group, Hersey, 2006, pp. 90-100.
[31] D.L. Tyler, C.M. Mulch, Interactive Wargaming Cyberwar: 2025, Thesis Dissertation, Naval Postgraduate School, Monterey, 2017.

[32] P.P. Perla, The Art and Science of Wargaming to Innovate and Educated in an Era of Strategic Competition, King's College London Wargaming Network Lecture, Video, 2018. URL: https://www.youtube.com/watch?v=rxLQmPA1-4o.
[33] E.M. Bartles, The Science of Wargames: A discussion of philosophies of science for research games, Presented at War Gaming and Implications for International Relations Research MIT CIS and US, Naval War College Workshop, Endicott House, Dedham. 2019. URL: http://www.elliebartels.com/uploads/1/1/0/6/110629149/bartels-the_science_of_wargames_nwc_mit.pdf.
[34] P.P. Perla, E. McGrady, Why Wargaming Works. Naval War College Review 64 (2011).
[35] B. Schechter, Wargaming Cyber Security, War on the Rocks, September 4, 2020. URL: https://warontherocks.com/2020/09/wargaming-cyber-security/.
[36] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Crossed Swords, n.d. URL: https://ccdcoe.org/exercises/crossed-swords/.
[37] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Locked Shields n.d. URL: https://ccdcoe.org/exercises/locked-shields/.
[38] E. Gartzke, J.R. Lindsay, Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace, Security Studies 24 (2015) 316-348.
[39] K. Zetter, Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon, Crown Publishers, New York, 2015.
[40] A. Liptak, The French Army is hiring science fiction writers to imagine future threats, The Verge, July 24, 2019. URL: ttps://www.theverge.com/2019/7/24/20708432/france-military-science-fiction-writers-red-team.
[41] Atlantic Council, Art of Future Warfare, n.d., URL: http://artoffuturewarfare.org/.
[42] United States Cyberspace Solarium Commission, Report, 2020. URL: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.
[43] N. Guilhot, Cyborg Pantocrator: International Relations Theory from decisionism to rational choice. Journal of the History of the Behavioral Science 47 (2011) 279-301.