Teaching Next-Generation Cyber Warfare

Jim Q. Chen
U.S. National Defense University, USA

drchen878@gmail.com

Abstract: Cyberspace plays a unique and crucial role in an era of a new geopolitical competition between the major powers. Cyber warfare has the flexibility of being launched either below or above the threshold of armed conflict in supporting the achievement of strategic goals and political aims. Meanwhile, cyber maneuvers are also inalienable to maneuvers in other warfighting domains such as land, maritime, air, and space. How can cyber capabilities be harnessed and integrated into joint warfighting? How can these new capabilities be taught to the joint force in a new way? These are the questions that the joint professional military education (JPME) programs should address. In the current JPME curricula, cyber capabilities are taught either in silo or in a way that is loosely connected to conventional military maneuvers. In a sense, they are not seamlessly integrated into the JPME programs. This paper addresses the issues of the current approach as well as their consequences. It intends to explore a new way of teaching next-generation cyber warfare, in which cyber capabilities are not only built into joint warfighting but also used to support the employment of relevant instruments of national power as well as the collaboration with allies and partners. This multi-level integrated approach is enabled by disruptive technologies such as artificial intelligence (AI). In so doing can cyber capabilities, especially AI-enabled cyber capabilities, be well integrated into the joint warfighting curricula, thus enabling joint force to obtain strategic advantage in the geopolitical competition.

Keywords: New Character of war, AI-Enabled Cyber, Joint Warfighting, Integration, Curricula

1. Introduction

In an era of a new geopolitical competition between the major powers, cyberspace plays a unique and crucial role since it can be used either below or above the threshold of armed conflict and it is inalienable to maneuvers in other warfighting domains such as land, maritime, air, and space. The flexibility makes cyberspace a suitable means in supporting the achievement of strategic goals and political aims. Hence, figuring out a new way of harnessing cyber capabilities and integrating them into joint warfighting is crucial.

As pointed out by the then Chairman of Joint Chiefs of Staff General Milley (2023), “Geostrategic competition and rapidly advancing technology are driving fundamental changes to the character of war.” “The rapid change in the character of war demands a corresponding fundamental shift in our Joint Force.” There are two tasks listed. One is to understand the new character of war. The other is to lead a change in the joint force. Of these two tasks, the first one drives the second one. In other words, without a deep understanding of the new character of war, it is hard to drive a shift in the joint force.

To understand the new character of war, one needs to understand at least the two major drivers of the change: geostrategic competition and rapidly advancing technologies.

The 2022 U.S. National Security Strategy mentions two strategic challenges that we are facing. “The first is that the post-Cold War era is definitively over and a competition is underway between the major powers to shape what comes next.” “The second is that while this competition is underway, people all over the world are struggling to cope with the effects of shared challenges that cross borders–whether it is climate change, food insecurity, communicable diseases, terrorism, energy shortage, or inflation.” These two strategic threads define the strategic environment that we are currently in, namely, competition in some areas while cooperation in other areas, or competition in some cases while cooperation in other cases. This requires the relevant nation-states to act within the spectrum of cooperation, coexistence, competition, and conflict.

The emerging technologies that contribute to the innovative and decisive military capabilities and capacities as well as military superiority involve artificial intelligence (AI) including machine learning (ML) and data analytics, robotics including drones, quantum computing, global positioning systems (GPS), etc. They, in turn, have made it possible for the development of ubiquitous sensors, analytical tools, new cryptographic tools, automated or autonomous vehicles and platforms, precision-guided munitions, long-range precision fires, advanced space capabilities, advanced cyber capabilities, just to list a few.

One may wonder what the character of war is. Milley (2023) further explains that it is about the way militaries conduct warfare. Specifically, it is about “how, where, with what weapons, and technologies wars are fought”. Specifically, in fighting a modern war, cyber, space, electromagnetic spectrum, and information capabilities should be integrated into the land, maritime, and air capabilities. Without this integration, a military force will

lose its eyes and ears as well as some critical capabilities in significant domains. This will make it almost impossible to win a war, or even to survive in a war.

It must be acknowledged that in the current JPME curricula, cyber capabilities are covered but not fully explored with respect to their role in joint warfighting. The skilful employment of cyber capabilities together with capabilities from other warfighting domains in a joint warfighting environment is seldom explored, not mentioning the strategies of their employment in joint warfighting. This, in a sense, fails in preparing the next-generation military leaders in dealing with the challenges in an environment in which the new character of war dominates. Thus, it can be claimed that cyber capabilities are not seamlessly integrated into the JPME programs at present.

One may wonder how cyber capabilities, especially AI-enabled cyber capabilities, can be harnessed and integrated into joint warfighting. One may also wonder how these new capabilities can be taught to the joint force in an JPME program. These are the questions that this paper intends to address.

This paper is structured as follows: Here in Section 1, the new character of war is briefly highlighted. So is the role that the cyber domain plays in joint warfighting. In Section 2, the issues of the current approach to cyber in the JPME programs are examined. In Section 3, a multi-level, multi-aspect, and integrated framework is established. This framework explicitly shows at which levels and in which aspects cyber capabilities can be integrated into capabilities of other domains and/or aspects. In this proposed approach, cyber capabilities are not only built into warfighting but also used to support the employment of relevant instruments of national power as well as the seamless collaboration with allies and partners. This multi-level, multi-aspect, and integrated approach is enabled by emerging technologies such as AI. In Section 4, the benefits of this framework are discussed. So is its implementation to improve the JPME education. Besides, future study is recommended. In Section 5, a conclusion is drawn.

2. Issues of the Current Approach to Cyber in the JPME Programs

The current curricula for the JPME programs were designed and developed for the warfare in the physical sphere, not for the hybrid warfare that involves the physical, virtual, and psychological spheres. Since the changing character of war is still emerging, the curricula lack the following components in general.

(1) The changing character of war is not well addressed in a holistic and systematic way in the current JPME curricula. Even though varied warfighting domains and varied instruments of national power are covered, a seamless integration of them is not, not mentioning the coverage of how to build and educate “an integrated and interoperable, multi-domain-capable, joint, and coalition force”, that is capable of “maneuvering through space and time in a fast-paced, high-tech, rapidly changing, and exceptionally challenging environment”, required in *Joint Publication 1 Volume 1 Joint Warfighting* by the U.S. Joint Chiefs of Staff (2023). In many cases, conflict and competition below the armed conflict are examined independently. Strategies in launching campaigns and operations in multiple domains and areas with allies and partners to achieve shared goals are not fully explored.

(2) The cyber domain is not prioritized in the current JPME curricula. In other words, the virtual battlefield is not emphasized. It is pointed out by Lonergan and Montgomery (2024) that “at root, the current readiness issue stem from the fact that none of the existing services prioritizes cyberspace.” Quoting a retired Navy captain, they note that this fundamental mismatch “has yielded varying levels of fragmented support to cyber operations, [a] lack of continuity of cyber personnel, unclear career paths, insufficient experience, wide use of non-cyber personnel in cyber leadership positions, and cyber operations being treated always as a supporting entity across all services”. This attitude is reflected in the current JPME education. Cyber capabilities are examined within the cyber domain. They are seldom explored together with capabilities in other warfighting domains. Hence, cyber is poorly integrated into joint warfighting. Consequently, modern warfighting is not investigated in a holistic and systematic way.

(3) In cyber force generation and development, specific domain knowledge, which is technical in nature, is required. Lonergan and Montgomery (2024) comment, “Manning and training for cyber operations are not equivalent to furnishing infantry or logistics personnel. All specialties have distinct training and skill requirements, but the cyber domain requires a uniquely high level of technical training.” As a result, how to effectively upskill senior leaders with sufficient cyber knowledge, especially AI-enabled cyber knowledge, is constantly a challenge. In the current JPME curricula, cyber fundamentals are covered. However, it is insufficient in teaching senior leaders how to harness AI-enabled cyber capabilities to fight and win both in cyberspace and

in conventional warfare. In this sense, the future leaders are not fully prepared in leading an integrated, interoperable, multi-domain-capable, joint and coalition force.

Force generation requires elegant organizing, effective training or education, and sufficient equipping. Missing any component will result in a failure. Therefore, a framework that connects cyber to other domains and aspects should be explored. Based on this framework, new way of teaching next-generation cyber warfare can be figured out. These topics are discussed in the following sections.

3. A Framework of AI-Enabled Cyber Engagement

Joint Publication 3-12 *Cyberspace Operations* defines cyberspace as the domain "that consists of the interdependent network of information technology (IT) infrastructures and resident data". Cyberspace "includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers". To put it in another way, cyberspace consists of hardware, software, firmware, internetworking systems, embedded processors and controller, and data. With the help of these systems, cyberspace is capable of engaging both the physical sphere and the virtual sphere. Since it can be used to influence humans, cyberspace is also capable of engaging the psychological sphere. Hence, it can be claimed that cyberspace sits on emerging and disruptive technologies since novel technologies in hardware, software, firmware, and internetworking systems, embedded processors and controller, and other innovative solutions are constantly being created and developed.

Likewise, AI is deeply rooted in cyberspace, as AI technologies are built on hardware, software, networking and communications systems, embedded processors and controllers, and other innovative solutions. In a sense, AI technologies further enhance the functions in cyberspace with respect to automation, autonomy, data analysis, decision-making, prediction, deception, and influence, thus further penetrating into the physical and psychological spheres. For instance, robotics (such as unmanned aerial vehicles (UVAs), unmanned surface vehicles (USVs), unmanned underwater vehicles (UUVs), and unmanned ground vehicles (UGVs)), Internet of Things (IoTs), and cyber-enabled industry control systems (ICSs) have helped to bring close together the virtual sphere and the physical sphere. Similarly, cyber-enabled information or influence campaigns have helped to bring close together the virtual sphere and the psychological sphere. Looking from this perspective, one may claim that AI has made cyberspace more powerful. In Joint Publication 3-12 *Cyberspace Operations*, it is stated, "Most aspects of joint operations rely in part on cyberspace". Cyberspace and AI are directly related, as the development and the use of AI applications heavily depends upon cyberspace. AI-enabled cyber can sufficiently bring close together the physical and virtual spheres by building physical hardware appliances operated with software and networking capabilities. Various robots are good examples. So are self-driving vehicles. Should cyberspace be enabled by AI, novel capabilities can be expected in bringing close together the physical, virtual, and psychological spheres. It is in this sense that AI-enabled cyber can be claimed to be an integrator of these spheres. Graphically, the relationship among AI-enabled cyber and the three spheres can be captured in Figure 1 below:

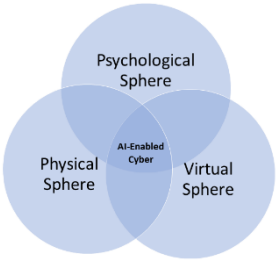

Figure 1: AI-Enabled Cyber - An Integrator of the Physical, Virtual, and Psychological Sphere

In modern warfighting, AI-enabled cyber can be a game-changer for command, control, communications, computer, cyber, intelligence, surveillance, and reconnaissance (i.e., C5ISR). According to the U.S. Army C5ISR Center, C5ISR can provide platforms "from Soldiers to ground vehicle, and from Air to Space". AI-enabled cyber thus "ensures our forces have the capability to see, sense, communicate, and move faster than our adversaries". In addition to the land domain, it can be employed to support C5ISR in the maritime, air, space, and cyber domains. Therefore, it can be argued that AI-enabled cyber can play a significant connectivity role in all warfighting domains.

As a contemporary war is conducted in the physical, virtual, and psychological spheres, emerging and disruptive technologies are required to support campaigns at different levels during different phases of war. In this sense, they are needed not only in joint warfighting that involves all domains, all instruments of national power, government agencies, international allies and partners, but also in unity of command or C3.

In examining deterrence in the contemporary age, Chen (2018a) explores levels of campaigns and operation both above and below the threshold of armed conflict. Chen and Dinerman (2018b) examine various types of cyber capabilities within these levels in modern warfare. Chen (2023) further proposes a multi-level and multi-aspect architecture that captures the escalation and de-escalation of conflict, the employment of multiple instruments of national power, and the engagement of alliances. All these levels cover the physical, virtual, and psychological spheres. Based on these studies, the author proposes a multi-level and multi-aspect framework of cyber engagement in competition and conflict. This framework is shown in Figure 2 below:

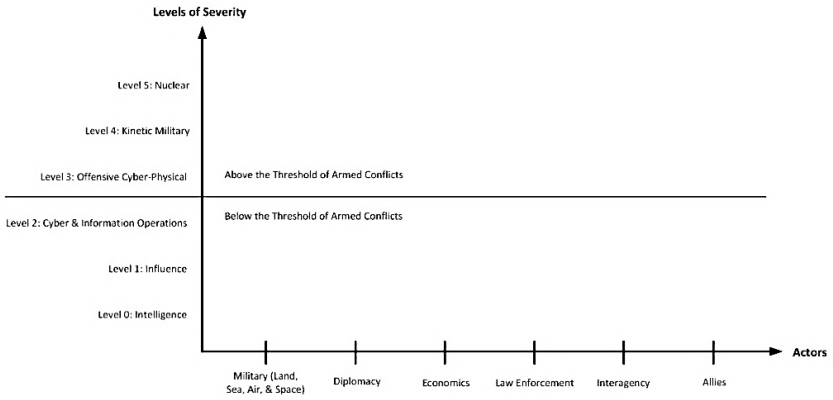

Figure 2: A Framework of Cyber Engagement in Competition and Conflict

This framework captures cyber engagement at various levels of competition and conflict. The vertical levels indicate levels of severity. The levels below the threshold of armed conflict are within the virtual and psychological spheres. The activities at these levels are for competition. The levels above the threshold of armed conflict are within the physical and virtual spheres. The campaigns and operations at those levels are for conflict.

The following levels are below the threshold of armed conflict:

- Level 0 is the level of intelligence collection and analysis operations.
- Level 1 is the level of influence campaigns.
- Level 2 is the level of cyber operations and cyber-enabled information operations.

The following levels are above the threshold of armed conflict:

- Level 3 is the level of offensive cyber-physical operations and campaigns.
- Level 4 is the level of kinetic or conventional military campaigns.
- Level 5 is the level of nuclear warfare.

Going from a lower level to a higher level indicates an escalation of a conflict, while going from a higher level to a lower level designates a de-escalation of a conflict. While in the physical sphere, AI-enabled cyber capabilities can be integrated into capabilities in the land, maritime, air, and space domains for joint campaigning and operations at each level of the framework.

At Level 0, intelligence can be collected in virtual and physical spheres via open-source intelligence collection methods, traditional intelligence collection methods, sensors, and other AI-enabled systems such as visual perception systems, image and facial recognition systems, speech recognition systems, natural language processing systems, machine translation systems, and decision-making systems. ML and data analytics can then be used to categorize the intelligence collected, figure out underlying trends of events, predict future development, and recommend courses of action (COAs).

At Level 1, cyber-enabled influence campaigns can be enhanced by AI in the virtual, physical, and psychological spheres. With AI-enabled deep fake capabilities in manipulating audio, video, images, and texts, the influence campaigns and information operations in social media and news media may confuse the targeted audience with misinformation and disinformation. Hageback and Hedblom (2022) list the following venues being used to

influence the targeted audience: media content, television, radio, music, movies, other entertainment means, websites, emails messages, and social media. Consequently, the targeted audience will be convinced of something false for a period of time, causing them to make wrong decisions before they realize the information that they receive and use for decision-making is false or inaccurate.

At Level 2, AI-enabled cyber capabilities can be used for offensive cyber operations, which include but are not limited to passive network attacks (such as wiretapping, fibre tapping, and port scan), passive host attacks (such as keystroke logging, setting up backdoor, and data scraping), active network attacks (such as distributed denial-of-service (DDoS) attacks, spoofing attacks, man-in-the-middle (MITM) attacks, and address resolution protocol (ARP) poisoning attacks), active host attacks (such as buffer overflow attacks, malware attacks, ransomware attacks, and data exfiltration attacks), social engineering attacks (such as phishing attacks and spear phishing attacks), database attacks (such as SQL injection attacks and cross-scripting attacks), cloud attacks, etc. AI can enhance these types of offensive operations with speed, stealth, and autonomy. Meanwhile, AI can enhance cyber defense in terms of malware detection, intrusion detection, intrusion prevention, and attack attribution.

Level 3 and above are engaged in conflict within the physical, virtual, psychological spheres. From the offensive perspective, AI-enabled cyber can play a significant role in offensive attacks against critical infrastructure (such as industry control systems (ICS) attacks, supervisory control and data acquisition (SCADA) system attacks, and Internet of Things (IoTs) system attacks) as well as weapon system attacks and logistic system attacks. From the defensive perspective, AI-enabled cyber can contribute greatly to the defense of these systems in terms of identification, prevention, detection, response, and recovery.

At Level 4, AI-enabled cyber can support kinetic or conventional military campaigns, especially the following principles of joint operations: offensive action, maneuver, economy of force, unity of command, surprise, and resilience. Specifically, in an offensive operation, AI-enabled cyber capabilities can be used to seize, retain, and exploit virtual targets. They can also be used to assist in seizing, retaining, and exploiting physical targets. UAVs, USVs, UUVs, UGVs, drone swarms, and other intelligent autonomous robotic devices can help to accomplish the military missions such as detection, deterrence, disruption, damage, and destruction. As observed by Husbands (2021), these robots are comprised of hardware devices (such as sensors and actuators) and software applications (such as perception, modelling, planning, motor commands, as well as analysis systems built on artificial neural networks). In maneuver, they can be utilized to put an adversary in a disadvantageous position virtually and physically. With the employment of human-machine teaming, minimum-essential human combat power is required, thus enabling economy of force. Furthermore, AI-enable cyber capabilities can be employed to support command, control, and communications (C3). Data analytics systems, visualization systems, and AI systems can visually project real-time data on environment as well as predictions and varied COAs to commanders in a unified format at dispersed locations, enhancing C3 capabilities. Being good at speed, precision, flexibility, anonymity, and stealth, AI-enabled capabilities can be used to launch unexpected strikes against virtual and physical targets, creating surprise effect for an adversary who is not prepared. As duplication is rapid in cyberspace, resilience can be easily set up in the virtual sphere. This enables the joint force to recover from loss quickly.

At Level 5, AI-enabled cyber capabilities can be used for nuclear warfare. As noted by Johnson (2021), technologies like AI, ML, and data analytics “have the potential to significantly improve the ability of militaries to locate, track, target, and destroy a rival’s nuclear-deterrent forces without the need to deploy nuclear weapons”. Besides, AI systems may “affect the dependability and survivability of nuclear command, control, and communications system” as well as the strategic decision-making process, since “AI-infused cyber capabilities may be used to manipulate, subvert, or otherwise compromise states’ nuclear assets”. In other words, AI-enabled or AI-augmented systems can create impact upon states’ nuclear deterrence force. In this sense, “AI applications that make survivable strategic forces, such as submarines and mobile missiles, more vulnerable (or perceived as such), could have destabilizing escalatory effects”. Likewise, Lieber and Press (2017) argue that AI and autonomy can enable real-time tracking and more accurate targeting of an adversary’s nuclear assets in ways that make counterforce operations more feasible. Meanwhile, speed, precision, flexibility, anonymity, and stealth that AI enjoys can further enhance the capability of nuclear weapons.

As shown above, AI-enabled cyber and information capabilities can be force-multipliers. They can be integrated into every level of the escalation ladder for military campaigns and operations. In addition, they can be integrated into other instruments of national power, such as diplomacy, economics, law enforcement, interagency collaboration, and cooperation with international allies.

In diplomacy, data analytics can be used to synthesize and analyze the data collected to have a better understanding of the current environment and the relationship among various events. AI can be used to figure out varied COAs in negotiation and then to select and recommend the most appropriate one to decision-makers. In economics, data analytics can be used to synthesize and analyze the economic and financial data. ML can help to find out the patterns as well as deviations from norms. Modelling and simulations can be utilized to examine the issues and to figure out varied solutions. AI can select the best solution and recommend it to decision-makers. For law enforcement, sensors and surveillance systems can be used to collect data. Data analytics systems can help to identify abnormal or suspicious activities and behaviour. AI systems can provide different COAs for selection. It can also select and recommend the most appropriate COA to decision-makers. In interagency collaboration and international allies' cooperation, AI systems can provide varied COAs, then select and recommend the most effective and efficient methods and measures, thus benefiting all the parties involved.

As shown above, the framework of cyber engagement in competition and conflict can seamlessly integrate AI-enabled cyber into other warfighting domains and instruments of national power.

Next, let us have a look at the benefits and implementation of the framework.

4. Benefits, Implementation, and Future Study of the Framework

In this section, the benefits of the framework are discussed. So are its implementation in helping to revise the JPME programs. Besides, the future study is recommended.

The framework enjoys the following benefits:

(1) Offering a holistic view: The framework elegantly brings together varied warfighting domains and instruments of national power. Since it takes into consideration both the levels below and the levels above the threshold of armed conflict, it provides a holistic view of the environment for decision-makers or commanders. Besides, it provides them with a platform for calculating the impact of a COA upon varied domains and aspects during a decision-making process.

(2) Adapting to the new character of war: By resorting to AI-enabled cyber capabilities, which are built on emerging and disruptive technologies, this framework makes it possible for each warfighting domain and each instrument of national power intricately linked together, thus combining the physical, virtual, and psychological spheres. This integration accelerates the adaptation to the new character of war via effectively employing cyber, space, electromagnetic spectrum, and information capabilities as well as emerging and disruptive technologies (such as AI, ML, and data analytics) at varied levels and in varied aspects to gain and maintain advantages in warfighting. In this way, the joint force will be accustomed to the new ways of fighting.

(3) Prioritizing the cyber domain: The framework provides the opportunity of having AI-enabled cyber capabilities seamlessly integrated into warfighting domains and instruments of national power. This can increase the role that the cyber domain plays in joint warfighting, thus prioritizing the cyber domain. This prioritization can help to ensure the continuity of highly technical and skilful cyber personnel, establish clear career paths, sufficiently employ AI-enabled cyber capabilities, greatly improve warfighting capabilities, thus laying the foundation for the joint force to effectively maneuver through the physical, virtual, and psychological spheres.

(4) Harnessing AI-enabled cyber capabilities: The framework makes it possible to harness AI-enabled cyber capabilities and utilize them in joint warfighting. Automation, autonomy, data analysis, decision-making, prediction, deception, and influence become available at each level and in each aspect with the help of the AI-enabled systems, such as sensing and surveillance systems, intelligence collection and analysis systems, risk assessment systems, cost-benefit analysis systems, impact analysis systems, decision-making systems, robotic systems, and other AI systems. As a result, the joint force can adapt to the new way of fighting, especially in the areas of offensive, maneuver, unity of command, security, surprise, and resilience, thus effectively maneuvering through the physical, virtual, and psychological spheres in the "fast-paced, high-tech, rapidly changing, and exceptionally challenging environment" (*Joint Publication 1 Volume 1 Joint Warfighting*, 2023).

Having a good understanding of the benefits of the framework can help us to figure out how to improve the current JPME curricula.

To develop future leaders and joint warfighters, *Joint Publication 1 Volume 1 Joint Warfighting* (2023) has mandated the revision of the JPME curricula "to develop strategically and operationally minded joint warfighters who can anticipate future joint warfighting, think critically, and creatively apply military power". Hence, in the JPME curricula, AI-enabled cyber, AI-augmented joint warfighting, and other emergent technologies that can be

integrated into each level and each aspect should be included, together with doctrines and leadership. Experiential learning and wargaming exercises should be used to enhance student learning.

Having these topics covered in the JPME programs can successfully address the issues of the current approach to cyber in the JPME programs, update the current JPME curricula to help students to gain a holistic view, adapt to the new character of war, prioritize the cyber domain in strategic decision-making, and harness AI-enabled cyber capabilities in campaign planning. Ultimately, it helps students to know how to fight and how to win in the hybrid warfare that consists of the physical, virtual, and psychological spheres.

Therefore, it is not sufficient to teach AI-enabled cyber warfare only within the cyber domain. It must be taught in the joint warfighting environment, in which AI-enabled cyber capabilities are closely integrated into every warfighting domain and every instrument of national power. This is the approach that should be adopted.

The research here outlines why the framework of cyber engagement in competition and conflict is needed, how it can be used to help develop the next-generation joint force, and what it can do in helping to revise the JPME curricula. Future study can be conducted to reveal the details of how AI-enable cyber capabilities are integrated into campaigns and operations in the land, maritime, air, and space domains. Besides, case studies and wargaming exercises on AI-enabled cyber capabilities and their integration into joint warfighting can be designed and developed to enhance student learning and joint force personnel development, thus helping the joint force in adapting to the new character of war and helping leaders to successfully lead a change in the joint force.

5. Conclusion

Geopolitical competition and rapidly advancing technologies have led to fundamental changes to the character of war. Contemporary warfare is conducted in the physical, virtual, and psychological spheres. AI-enabled capabilities, which engages all three spheres, can serve as an integrator of these spheres. Besides, AI-enabled cyber can be a force multiplier, as it consists of the unique characteristics such as speed, precision, flexibility, anonymity, stealth, low-cost, hit-and-run, and others. To show the roles that AI-enabled cyber can play in joint warfighting and other national security missions, this paper proposes the framework of cyber engagement in competition and conflict. This framework categorizes cyber engagement or maneuvers below or above the threshold of armed conflict at varied levels and in varied aspects. It also reveals that AI-enabled cyber capabilities can be integrated into other warfighting domains and instruments of national powers. It argues that the next-generation AI-enabled cyber warfare should be taught in this way.

After examining the issues of the current approach to cyber in the JPME programs, the paper proposes the framework that can integrate AI-enabled cyber capabilities into joint warfighting and that can improve the JPME curricula by effectively addressing the issues. Thus, it helps the joint force to adapt to the new character of war and gain strategic advantage in the geopolitical competition.

References

Chen, J. (2023) “Deterrence in Cyberspace: An Essential Component in Integrated Deterrence”, *Integrated Deterrence and Cyberspace*, Joseph Billingsley (ed.), pp.1-21. Washington DC, USA: The National Defense University Press.

Chen, J. (2018a) “On Levels of Deterrence in the Cyber Domain”, *Journal of Information Warfare*, Vol.17, 2, pp.32-41.

Chen, J. and Dinerman, A. (2018b) “Cyber Capabilities in Modern Warfare”, *Cyber Security: Power and Technology*, M. Lehto and P. Neittaanmäki (eds.), pp.21–30. Springer.

Hageback, N. and Hedblom, D. (2022) *AI for Digital Warfare*, Oxon, UK: CRC Press.

Husbands, P. (2021) *Robots: What Everyone Needs to Know*, Oxford, UK: Oxford University Press.

Johnson, J. (2021) *Artificial Intelligence and the Future of Warfare*, Manchester, UK: Manchester University Press.

Lonergan, E. and Montgomery, M. (2024) “United States Cyber Force: A Defense Imperative”, Washington DC, USA: Foundation for Defense of Democracies (FSS) Press.

Lieber, K. and Press, D. (2017) “The New Era of Counterforce: Technological Changes and the Future of Nuclear Deterrence,” *International Security*, Vol.41, 4, pp.9-49.

Milley, M. (2023) “Strategic Inflection Point: The Most Historically Significant and Fundamental Change in the Character of War Is Happening Now–While the Future Is Clouded in Mist and Uncertainty”, *Joint Force Quarterly,* Volume 110, 3rd Quarter, pp.6–15, Washington DC, USA: the NDU Press.

The U.S. Army C5ISR Center (2024) “Combat Capabilities Development Command C5ISR Center”. Retrieved from c5isrcenter.devcom.army.mil.

The Joint Chiefs of Staff. (2023) *Joint Publication 1 Volume 1 Joint Warfighting*, Washington DC, USA.

The Joint Chiefs of Staff. (2018) *Joint Publication 3-12 Cyberspace Operations*, Washington DC, USA.

The Joint Chiefs of Staff. (2011) *Joint Publication 3-0: Joint Operations*, Washington DC, USA.

The White House. (2022) *U.S. National Security Strategy*, Washington DC, USA.