6

Artificial Intelligence in Cyber Peace

Tabrez Y. Ebrahim

1 INTRODUCTION

This chapter examines artificial intelligence (AI, i.e., or mathematical models for representing computer problems and algorithms for finding solutions to these problems) and its impacts on an arms race (i.e., each nation is focused on self-interest in seeking an incremental gain over another for technological superiority of weapons) (Craig & Valeriano, 2016, p. 142). In the absence of cooperation, all nations are worse off than if they would be if they cooperated in some form. This chapter overviews how AI's unique technological characteristics – including speed, scale, automation, and anonymity – could promote an arms race toward cyber singularity (i.e., a hypothetical point where AI achieves Artificial General Intelligence (AGI), that surpasses human intelligence to become uncontrollable and irreversible) (Newman, 2019, p. 8; Priyadarshini & Cotton, 2020). AI technological advancements have generated a good deal of attention about the AI arms race and its potential for producing revolutionary military applications. While the AI arms race has raised implications for cyber peace, a less studied issue is the potential impact on AGI development in cybersecurity, or cyber singularity. While there is some hype and a development time period toward cyber singularity, the results are generally viewed as negative or, at worst, destabilizing or even catastrophic for cyber peace.

Notwithstanding such limitations, there is still huge potential for the use of technological advancements in AI for civilian, consumer-focused applications, and for the inevitable advancements in nations' military and security technologies. Economic competition for AI has already motivated its development and implementation by the private sector. This has contributed to the imbalance of the economic dominance by industrialized countries. Innovative companies and countries that focus on AI development may begin to monopolize AI knowledge and take the lead toward cyber singularity, which could thwart cyber peace. AI has also become an essential component of cybersecurity, as it has become a tool used by both attackers and defenders alike (Roff, 2017). In the future, the more advanced form of AGI, or super technological intelligence, could develop its own understanding of the

https://doi.org/10.1017/9781108954341.006 Published online by Cambridge University Press

world and react to it in a rapid and uncontrollable way without human involvement. Advancement toward cyber singularity could present new military capabilities, such as manipulation of data and overcoming other nations' defenses, and transform interactions in cyber conflict. While is difficult to detect or measure the origination or proliferation of AI in cybersecurity, whatever possible cooperation among nations that can be promoted is certainly worth exploring. Thus, this chapter explores how shared governance through talent mobilization in the form of a global AI service corps can offset the negative impact of nation-states' economic competition to develop AGI.

2 BACKGROUND AND CHARACTERIZATION OF AI

The definition of AI varies in context and is a moving target as technology continues to advance (Lemley & Case, 2020, p. 1). The term AI is meant to refer to computer programs that perform mathematically oriented tasks that were generally assumed to require human intelligence (Lefkowitz, 2019). AI can take a variety of forms including logical inference (a form of deduction) and statistical inference (of form of induction or prediction) (Eldred, 2019). Such mathematical techniques are becoming more powerful because of the availability and use of large datasets, easy access to powerful and inexpensive computing resources, and the ability to run new algorithms and solve complex problems using massive parallel computing resources (Firth-Butterfield & Chae, 2018, p. 5; Daly, 2019). Another way to look at the current state of AI is that it has become cheaper and easier to utilize its techniques with more speed, scale, and automation than ever before. Moreover, the platforms of collecting, using, and solving relationships in data can be done anonymously, which presents opportunities for exploitation of consumers in business and nations in cyber conflict.

Technological advancements have always played a crucial role in the context of conflict and peace (Roff, 2016, p. 15). The introduction of information technology presented opportunities to create, move, and process data in ways never seen before, leaving nations with the power to control, defend, secure, and weaponize data. AI performs these tasks better, faster, and with more anonymity than humans, and outperforms ordinary computers and networked systems.

The information technology sophistication of AI allows for disguised and stealth measures, provides for more effective and contextualized threats, and has the potential for amplified human cognitive capabilities in the form of cyber singularity over time (Priyadarshini & Cotton, 2020). Many characteristics of information technology – including its ability to involve multiple actors, attribute challenges, and proliferate across borders – present unprecedented challenges for AI in cyber peace (Geers, 2011, p. 94). Information technology warfare and protection measures in the modern day present unique considerations for AI compared to prior means and methods. In this vein, AI-based information technologies related to cyber peace fall

into three primary classifications: (1) information attacks; (2) information anonymity; and (3) information attribution (Reuter, 2020, p. 16, 24–5, 113–14, 117, 279–81). A new classification of manipulation or change by AI, which is increasingly becoming ubiquitous, presents new opportunities for the integration of multiple stakeholder input.

With AI, nations can analyze patterns and learn from them to conduct cyberattacks (i.e., offensive capabilities of AI) and also use these patterns prevent cyberattacks (i.e., defensive capabilities of AI) in more advanced mechanisms than current capabilities. The state of the art AI already allows for discovering of hidden patterns in data and automating and scaling mathematical techniques with data to make predictions (Coglianese & Lehr, 2018, pp. 14–15).

The path toward AGI is especially attractive insofar as it will not seem to require human intervention and will control the information infrastructure in cyber conflicts (Burton & Soare, 2019, pp. 5–6). As the tools, techniques, and software become increasingly intelligent, AI will have greater role in cyber conflict and cyber peace. To assess this path toward AGI and its implications for shared governance, an overview of information security technology and AI's role in information security is necessary as a preliminary matter.

2.1 *Information Security Overview*

The stakes in our national information security debate are high. Information security refers to the hybrid scientific and legal inquiry into defending against all possible third-party attackers and the legal consequences that arise when they cannot. The purpose of information security is to develop and provide technological solutions to prevent the potential for cyberattacks and to minimize the interstate insecurity caused by information technologies (Libicki, 2009, pp. 12–13). Information security technologies have a crucial impact on AI's role in cyber peace, and therefore, it is necessary to have a proper understanding of what these concepts mean and how they may accelerate or decelerate concerns for a path toward a sustainable and secure cyber peace.

Information security is a capricious concept with varying definitions in the legal and policy realms, but it has a more concrete meaning in computer science and technological realms (Reuter, 2020, pp. 17–18). In a technological sense, the cyber world of computerized networks where information technologies are relevant have three layers: (1) a physical layer of infrastructure (including integrated circuits, processors, storage devices, and optical fibers); (2) a software logic layer (including computer programs and stored information that is subject to processing); and (3) a data layer, for which a machine contains and creates information (Tabansky, 2011, p. 77). In order to analyze the relevance of information technology, particularly AI, and its role in cyber peace, it is necessary to understand how these concepts relate to technology characteristics. While conflicts among nations can be carried out in different domains, such as land, sea, air, and space, conflict with the use of

information technology infrastructure has the following peculiar characteristics for security implications: (1) many actors can be involved; (2) the identity of the security threat may be unknown due to the challenge of attribution; (3) international proliferation; and (4) its dual-use nature that can be exploited in a variety of ways (Reuter, 2020, pp. 12–13). These characteristics are accounted for in the various defensive and offensive uses of information technology, as subsequently shown.

2.2 *Defensive Information Security Measures*

Defensive protection measures allow for proactive ways to detect and obtain information regarding cyberattacks or intrusion (Chesney, 2020, p. 3). Defending against cyberattackers entails the use of software tools that obfuscate or obscure cyberattackers' efforts (Andress & Winterfeld, 2011, p. 113). A major goal of defensive cyber protection is to prevent critical infrastructure damage which would generate large spillover effects in the wider economy. The defensive cyber protection approach seeks to: (i) minimize unauthorized access, disruption, manipulation, and damage to computers and (ii) mitigate the harm when such malicious activity occurs to computers. In so doing, information security seeks to preserve the confidentiality, integrity, and availability of information (Tabansky, 2011, p. 81).

Approaches fall into two general categories: proactive measures (also known as preventative techniques, which can block efforts to reach a vulnerable system via firewalls, access controls, and cryptographic protection) and deterrence measures (that increases the effort needed by an adversary, and includes many types of security controls) (Ledner et al., 2009, pp. 6–7, 9–10). In either approach, the goal is to prevent unauthorized access to a computer system by the use of technological methods to identify an unauthorized intrusion, locate the source of the problem, assess the damage, prevent the spread of the damage, and reconstruct damaged data and computers (Reuter, 2020, pp. 22, 280–283). Deterrence, mitigation, and preventative strikes with the use of information technology include application security, attack detection and prevention, authorization and access control, authentication and identification, logging, data backup, network security, and secure mobile gateways.

2.3 *Offensive Information Security Measures*

While defensive measures and technology can deter and mitigate the consequences of unauthorized access of computers and networks, limiting unauthorized access may not achieve cyber policy goals. Offensive measures, which are considered lawful but unauthorized, refer to penetrating or interfering with another system and can include mechanisms that allow for impersonation of trusted users and faster attacks with more effective consequences (Dixon & Eagan, 2019). Such offensive measures are one of many ways that nations can utilize cyber power to destroy or disable an adversary's infrastructure (Voo et al., 2020). Nations seek to achieve cybersecurity

in order to bend the other side's will or to manage the limiting the scope of the other side's efforts, and can do so, via deliberate provocation or through escalation via offensive measures or cyberattacks (Jensen, 2009, pp. 1536–1538). A common mechanism for cyberattacks is a computer network attack, wherein actions are taken through the use of information technology and computer networks to disrupt, deny, degrade, or destroy information on computers and networks, and can electronically render useless systems and infrastructures (Andress & Winterfeld, 2011, pp. 110–113).

The increasing power of computers, proliferation of data, and advancements in software for AI capabilities presents many new applications of offensive measures. To demonstrate that AI is a rapidly growing field with potentially significant implications for cyber peace, several technological examples are provided to show the direct or indirect impact of such technological advancement on the need for *shared governance of a global service AI corps*.

Attack means and methods include malware, ransomware, social engineering, advanced persistent threats, spam, botnets, distributed denial of service, drive-by-exploits and exploit kits, identity theft, and side channel attacks. Such cyberattacks include the intrusion of the digital device with some sort of malware that initiates the communication between the attacking computing and the intruded device. The reasons for initiating such offensive measures include preventing authorized users from accessing a computer or information service (termed a denial-of-service attack) destroying computer-controlled machinery, or destroying or altering critical data and, in doing so, can affect artifacts connected to systems and networks (such as cyber-physical devices, including generators, radar systems, and physical control devices for airplanes, cars, and chemical manufacturing plants). Cyberattack mechanisms include the use of malware installation (sometimes combined with disruptive code and logic bombs), creation of botnets (that refer to a group of infected and controlled machines that send automated and senseless reports to a target computer), and installation of ransomware (that encrypts a device) (Reuter, 2020, pp. 16, 24–5, 113–14, 117, 140, 279–81). Malware refers to malicious software, which can attack, intrude, spy on, or manipulate computers. Botnets are made up of vast numbers of compromised computers that have been infected with malicious code and can be remotely controlled through Internet-based commands. Ransomware refers to malicious software that is installed on a computer, network, or service for extortion purposes, by encrypting the victim's data or systems and making them unreadable such that the victim has to submit a monetary payment for decrypting files or regaining access.

2.4 *Information Security Linkage to Artificial Intelligence*

Technological development, particularly in the rapidly developing information technology realm, plays a crucial role in questions regarding cyber peace. Information technology is becoming omnipresent in the cases of resilience and of

https://doi.org/10.1017/9781108954341.006 Published online by Cambridge University Press

managing cyber conflicts. As the interdisciplinary field of cyber peace links more with technology, it is crucial to consider the ways that information technology assists and supports peace processes, as well as be cognizant of ways it can be a detriment.

Ever since information technology has created, moved, and processed data, the security of the data encountered challenges with policy and conflict resolution. In recent years, as advancements in information technology have increased connectivity, collaboration, and intelligence, these issues have become even more important. Information technology concerns information sharing and deterrence and implicates security concerns. As such, information technology security involves the preservation of confidentiality, integrity, availability, authenticity, accountability, and reliability. Relatedly, information technology can manipulate and anonymize data, and this feature can be used for a cyberattack (Gisel & Olejnik, 2008, pp. 14–17). The implication of this capability is attribution challenges. Attribution refers to the allocation of a cyberattack to a certain attacker toward providing real-world evidence for unveiling the identity of the attacker. AI makes it easier to identify or attribute a cyberattacker since it analyzes significantly higher number of attack indicators and discovers patterns (Payne, 2018).

AI is poised to revolutionize cyber technological use in cyber peace, by providing faster, more precise, and more disruptive and anomalous capabilities (Stevens, 2020, pp. 1, 3, 4). AI can analyze data and trends to identify potential cyberattacks and provide offensive countermeasures to such attacks (Padrón & Ojeda-Castro, 2017, p. 4208). Moreover, AI presents the most powerful defensive capability in cybersecurity (Haney, 2020, p. 3). While AI presents new technological capabilities to cyber conflict, it raises new considerations of what it might mean for human control, or lack thereof, and how it may help or hinder risks (Burton & Soare, 2019, pp. 3–4). AI capabilities can undermine data integrity and present stealthy attacks that cause trust in organizations to falter and lead to systemic failures (Congressional Research Service, 2020, Summary). Nations could use AI to penetrate another nation's computers or networks for the purposes of causing damage or disruption through manipulation and change (Taddeo & Floridi, 2018, pp. 1–2).

From an offensive standpoint, AI presents new considerations for cyber conflict, such as new manipulation or change capabilities that can allow for expert compromise of computer systems with minimal detection (Burton & Soare, 2019, pp. 9–10). Adversarial AI impacts cyber conflict in three ways, including impersonation of trusted users, blending in the background by disguise and spreading itself in the digital environment, and faster attacks with more effective consequences. These capabilities provide motivation for the "defend forward" strategy of a preemptive instead of a reactive response to cyberattacks (Kosseff, 2019, p. 3).

Additionally, AI makes deterrence possible since its algorithms can identify and neutralize the source without necessarily identifying the actor behind it, which makes it easier to thwart attacks. AI capabilities allow for going to the forefront of

the cause or the conflict to analyze data and trends to identify potential attacks and provide countermeasures to such attacks.

3 PATH TOWARD AGI AND IMPLICATIONS FOR CYBER SINGULARITY

The technological development and advancement of AI presents challenges and lessons for governance frameworks. Social science research has been applied toward addressing governance gaps with AI, including polycentric governance and the resulting implications for policymakers (Shackelford & Dockery, 2019, pp. 6–7; Shackelford, 2014, pp. 2, 4–5).

There is no single definition of AGI, but the general consensus is that AGI refers to machines gaining intelligence that is greater than that of humans (Payne, 2018). When AGI is applied to cybersecurity, it has been termed cyber singularity, which presents superintelligence and amplification of human cognitive capabilities in cyberspace. The path toward AGI involves advancements in the form of a technological tool in a classical scenario and in the application of such a tool in novel situations.

The race to AGI involves the development of tools (mathematical techniques and software) used in classical cyber offense and cyber defense scenarios, but with increasing intelligence (Burton & Soare, 2019, pp. 5–6). These represent technological attacks on computer networks, data, and infrastructure. While achieving AGI is a futuristic concept, advancements in sensory perception and natural language understanding will help transform AI into AGI and present new offensive and defensive capabilities in cyber peace. The offensive capabilities of AGI could involve sabotaging data, masking and hiding it being a cyberattack, and engaging in changing behaviors and contextualizing its threats. The defensive capabilities of AGI could involve automatically scanning for vulnerabilities in computer networks, gathering intelligence through the scanning of computer systems, and improving existing software and scripts. In both the offensive and defensive realm, AGI could manipulate humans or detect when humans were being manipulated and respond accordingly. Similar to an advanced form of psychological manipulation of behavioral advertising, AGI could conduct sophisticated manipulation of human decision-making in the midst of a cyber conflict and, in doing so, could amplify points of attack, coordinate resources, or stage attacks at scale (National Science & Technology Council, 2020, p. 7).

The race toward AGI also involves application of such tools in novel forms pertaining to cybersecurity (Geist, 2016; Cave & ÓhÉigeartaigh, 2018). In additional to technological attacks on computer networks, data, and infrastructure, AGI could be applied to psychological manipulation in society to shape information in the political realm, the Internet, and social media with national cybersecurity implications. In the context of cybersecurity, AGI, as applied to manipulation of people with societal impact, includes shaping public understanding and political action that

impacts national cybersecurity policy. Unlike the scenario of AGI as a technological tool, in a related manner, AGI as socio-political manipulator can provide an automated mass deception or mass data collection that implicates national cybersecurity and global perspectives. While not as direct an impact as a technological attack on computer networks, data, and infrastructure, this form of AGI provides manipulative messaging and interference in media, politics, and the public sphere, akin to the profiling and data analysis methods implemented in the Cambridge Analytica scandal.

In addition to the advancement of AI toward AGI for use as a technological tool, and its application to shape the socio-political information realm, AGI technological advancement in the form of cyber singularity would necessitate transformation of warfare approaches (Ivey, 2020, p. 110; O'Hanlon, 2018). Cyber singularity, or the hypothetical point of AGI, becomes uncontrollable and irreversible in the cybersecurity realm and implicates international initiatives and policies (Priyadarshini & Cotton, 2020). The literal interpretation of cyber singularity concerns targeting weapons advancement with an offset strategy, or achieving technological superiority for deterrence effects. Similar to past offset strategies with nuclear weapons and information surveillance and stealth weapons, AGI for cyber singularity represents the next offset strategy. The strategic development and use of modern algorithms, data, and information on computer networks in the path toward AGI is critical in the AI arms race. In this sense, the world is at a critical stage in the strategic use of data and control of information on computer networks. As nations seek AGI capabilities in the AI arms race, policies that promote its development are of critical importance. A shared governance approach in some form should consider ways to offset the negative impact of nation-states' economic competition to develop AGI.

4 SHARED GOVERNANCE OF A GLOBAL SERVICE AI CORPS

The idea about the path toward AGI and implications of cyber singularity is that it might be possible to create a computational machine that vastly outperforms humans in cognitive areas of cybersecurity. Whereas current state of the art AI can apply to limited cybersecurity domains, AGI could also learn and expand into more cyber domains. The potential for AGI is speculative and the idea of cyber singularity is fuzzy since it is unclear what technologies are necessary for its realization. Thus, with an unclear understanding of the likelihood and function of cyber singularity, the technological development pathway raises a host of questions. By contrast, nations could foreseeably control governance strategies in relation to AGI. One potential option – that this chapter prescribes – is directing talent and human resources toward cooperation.

Nations that direct human capital resources in this way would allow for exerting control of human behavior in the arms race toward AGI and implications toward cyber singularity. Currently, there is a "brain drain" of AI talent that is largely employed

by the private sector (Andress & Winterfeld, 2011, p. 248; Congressional Research Service, 2009, p. 22). A commission that recruits, develops, and retains AI talent, such as in the form of a reserve corps, could help to equalize the playing field in the AI arms race and transform governance away from state-centric approaches to AI. The facilitation of early global coordination among multiple stakeholders with common interests and sharing of best practices could prevent global catastrophic cybersecurity risks (Newman, 2019, p. 4). Such a multistakeholder policy toward AI development represents a system flexible enough to adapt to new challenges and realities in a global system and toward cyber peace, potentially even forming the backbone of a Cyber Peace Corps (Shackelford, 2017). Given that AI technological development toward AGI has been under the purview of nations, the solution to the problem of an AI arms race toward cyber singularity needs to be rooted through multilateral networks.

The AI arms race has largely been framed by its economic impact rather than in shared governance structures. As a result, industrialized countries with strong software industries have continued to develop AI tools that have skewed the AI arms race. As AI and data implicate economic wealth and political influence, cyber peace policy conversations will need to consider the role and advancement of AI. The greatest threat to and the greatest opportunity for cyber peace could be AI technology, rather than other forces in the nations themselves.

REFERENCES

Andress, J., & Winterfeld, S. (2011). *Cyber warfare*. Elsevier.

Burton, J., & Soare, S. (2019). *Understanding the strategic implications of the weaponization of artificial intelligence* [Manuscript]. 11th international conference on cyber conflict. Tallinn, Estonia. https://ccdcoe.org/uploads/2019/06/Art_14_Understanding-the-Strategic-Implications.pdf

Cave, S., & ÓhÉigeartaigh, S. (2018, December). *An AI race for strategic advantage: Rhetoric and risks*. AIES '18: Proceedings of the 2018 AAAI/ACM conference on AI, ethics, and society. New Orleans, LA, USA. https://doi.org/10.1145/3278721.3278780

Chesney, B. (2020, March 2). *Cybersecurity law, policy, and institutions, v.3.0*.

Congressional Research Service. (2020, August 26). *Artificial intelligence and national security*.

Congressional Research Service. (2009, March 17). *Information operations, cyberwarfare, and cybersecurity: Capabilities and related policy issues*.

Coglianese, C., & Lehr, D. (2018, November 9). Transparency and Algorithmic Governance. *Administrative Law Review, 71*(1), 1–56.

Craig, A. & Valeriano, B. (2016). *Conceptualising cyber arms races* [Manuscript]. 8th International conference on cyber conflict. Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

Daly, A. (2019, June 5). *Artificial intelligence governance and ethics: Global perspectives*. https://arxiv.org/ftp/arxiv/papers/1907/1907.03848.pdf

Dixon, W., & Eagan, N. (2019, June 19). *3 Ways AI will change the nature of cyber attacks*. World Economic Forum. www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

Eldred, C. (2019, October). *AI and domain knowledge: Implications of the limits of statistical inference*. Berkeley Roundtable on International Economics. https://brie.berkeley.edu/sites/default/files/ai_essay_final_10.15.19.pdf

Firth-Butterfield, K., & Chae, Y. (2018, April). *Artificial intelligence collides with patent law*. World Economic Forum. www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf

Geers, K. (2011, January 1). *Strategic cyber security*. NATO Cooperative Cyber Defence Centre for Excellence.

Geist, E. M. (2016, August 15). It's already too late to stop the AI arms race—we must manage it instead. *Bulletin of the Atomic Scientists*, *72*(5), 318–321. https://doi.org/10.1080/00963402.2016.1216672

Gisel, L., & Olejnik, L. (2008, November 14–16). *The potential human cost of cyber operations* [Manuscript]. ICRC Expert Meeting. Geneva, Switzerland. www.icrc.org/en/document/potential-human-cost-cyber-operations

Haney, B. S. (2020). Applied artificial intelligence in modern warfare & national security policy. *Hastings Science and Technology Journal*, *11*(1), 61–100.

Ivey, M. (2020). The ethical midfield in artificial intelligence: Practical reflections for national security lawyers. *The Georgetown Journal of Legal Ethics*, *33*(109), 109–138. www.law.georgetown.edu/legal-ethics-journal/wp-content/uploads/sites/24/2020/01/GT-GJLE190067.pdf

Jensen, E. T. (2009). Cyber warfare and precautions against the effects of attacks. *Texas Law Review*, *88*(1533), 1534–1569.

Kosseff, J. (2019). *The countours of 'Defend Forward' under international law*, 2019 11th International Conference on Cyber Conflict (CyCon) 900, 1–13.

Ledner, F., Werner, T., & Martini P. (2009). Proactive botnet countermeasures – An offensive approach. In C.Czosseck & K.Geers (Eds.), *The virtual battlefield: Perspectives on cyber warfare* (pp. 211–225). 10.3233/978-1-60750-060-5-211

Lefkowitz, M. (2019, September 25). *Professor's perceptron paved the way for AI – 60 years too soon*. Cornell Chronicle. https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way-ai-60-years-too-soon

Lemley, M. A., & Case, B. (2020). You might be a robot. *Cornell Law Review*, *105*(287), 287–362.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.

National Science & Technology Council. (2020, March). Networking & Information Technology Research and Development Subcomittee and the Machine Learning & Artificial Intelligence Subcommittee. Artificial Intelligence and Cybersecurity: Opportunities and Challenges, Technical Workshop Summary Report.

Newman, J. C. (2019, February). *Towards AI security: Global aspirations for a more resilient future*. Center for Long-Term Cybersecurity.

O'Hanlon, M. E. (2018, November 29). *The role of AI in future warfare*. Brookings. www.brookings.edu/research/ai-and-future-warfare/

Padrón, J. M., & Ojeda-Castro, Á. (2017, June). Cyberwarfare: Artificial intelligence in the frontlines of combat. *International Journal of Information Research and Review*, *4*(6), 4208–4212.

Payne, K. (2018). *Artificial intelligence: A revolution in strategic affairs?* International Institute for Strategic Studies.

Priyadarshini, I., & Cotton, C. (2020, May 6). Intelligence in cyberspace: The road to cyber singularity. *Journal of Experimental & Theoretical Artificial Intelligence*. https://doi.org/10.1080/0952813X.2020.1784296

Reuter, C. (2020). *Information technology for peace and security*. Springer.

Roff, H. M. (2016, March). *Cyber peace, new America*. Cybersecurity Initiative.

Roff, H. M. (2017, August 1–3). *Cybersecurity, artificial intelligence, and nuclear modernization* [Workshop]. Cyberwarfare and Artificial Intelligence. University of Iceland, Reykjavik, Iceland.

Shackelford, S. J. (2014, April 16). Governing the final frontier: A polycentric approach to managing space weaponization and debris. *American Business Law Journal*, 51(2), 429–513.

Shackelford, S. J. & Dockery, R. (2019, October 30). Governing AI. *Cornell Journal of Law and Policy*. Advanced online publication.

Stevens, T. (2020, March 31). Knowledge in the grey zone: AI and cybersecurity. *Journal of Digital War*. https://doi.org/10.1057/s42984-020-00007w

Tabansky, L. (2011, May). Basic concepts in cyber warfare. *Military and Strategic Affairs*, 3(1), 75–92.

Taddeo, M., & Floridi, L. (2018, April 16). Regulate artificial intelligence to avert cyber arms race. *Nature*, 556(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020, September). *National Cyber Power Index 2020*. Belfer Center for Science and International Affairs, Cambridge, Tech. Rep. September 2020 [Online]. Available: www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf