Santa Clara Journal of International Law

Volume 18 | Issue 1 Article 3

1-10-2020

Coming to a Battlefield Near You: Quantum Computing, Artificial Intelligence, & Machine Learning's Impact on Proportionality

Salahudin Ali

Coming to a Battlefield Near You: Quantum Computing, Artificial Intelligence, & Machine Learning's Impact on Proportionality

Salahudin Ali*+

* Judge Advocate, USMC. LL.M., 2018, The Scalia School of Law at George Mason University; J.D., 2011, Lewis & Clark Law School. The comments in this article are those of the author and are not associated with the Department of Defense or any other government agency. All errors are my own.

+ All sources used herein for the purposes of this article are unclassified or declassified. The author understands that the existence of classified sources may impact the article's analysis.

Abstract:

No invention by nature is inherently disruptive, instead, it must be used disruptively. This is especially true when advanced technologies intersect with standards of industry practice. Conflicts between nations being no exception. In war, those principles and standards of practice are governed by a complex set of normative behaviors and signed agreements both reflected in the law of armed conflict and customary international law.

The principle of proportionality will be impacted by a new, advanced technology that implements quantum computing, artificial intelligence, and machine learning for purposes of advanced decision-making and increased computing speed and accuracy. This technological iconoclasm may disrupt the mental assurance requirements that drives decision-makers' targeting analysis for purposes of accomplishing military objectives, and the destructive results that follow such decisions. This is due to the opaqueness of such technologies, the battlefield—the cyber domain, as well as a lack of clarity in legal nomenclature regarding the principle itself.

This article examines such impacts and analyzes how mental assurance requirements may not be met if there is a misunderstanding as to how and why a technology makes decisions; and if there is a misunderstanding of the level of damage caused by such technology. It also examines legal interpretations and past uses of advanced technologies in the cyber domain, and how they can provide a way forward in crafting useful solutions to this approaching reality.

Consequently, the opaqueness of such technology must be reconciled with new governing principles. This article concludes that a more proactive approach in understanding technological development, clarity in legal terms, and responsible decision-making cycles ensure use of such technologies on a legally sufficient basis.

"Accidents happen. That's what everyone says.
But in a quantum universe there are no such
things as accidents, only possibilities and
probabilities folded into existence by perception." –Dr. Manhattan

"When you change the way you look at things,
the things you look at change."-Max Planck

Table of Contents

I. Introduction

A. Hypothetical

Let's picture a scenario where: An operational planning team convenes a targeting board to conduct analysis for an attack on adversary command-and-control systems. Due to the adversary's technological sophistication and its integrated national economy, the enemy's communication infrastructure has allowed current success in coordinating its movement of forces on the battlefield. The targeting board concludes that without this coordination, the adversary could not operate successfully—it is a critical vulnerability.[1] A decision is made to use a new weapon system that combines artificial intelligence (AI)[2], machine learning (ML),[3] and quantum computing (QC)[4] technologies and methodologies to disable enemy communication systems that allow this coordination. This enemy communication system is comingled via internet infrastructure with the country's civilian communication network serving as its underlying foundation. The new platform quickly decides that disabling the entire network system of the country—including those aspects outside of this conflict zone—will achieve a decisive decision leading to an end to the conflict. It promptly uses quantum computing methodologies to access, decrypt, disable, and adversely re-encrypt the entire nation-state's communication system, rendering it inoperable by said-named nation state and depriving the nation state's citizens of their national and political economy for undetermined period of time. The infrastructure also has suffered physical damage as there is no ability to conduct troubleshooting or maintenance for its recovery.

B. Framework and Disruption

"[N]o invention is innately 'disruptive'…it must be used disruptively,"[5] as noted by Russian chestmaster, Garry Kasparov. This is especially true when advanced technologies intersect with principles and standards of practice of an industry. Conflict between nations is no exception. In war, those principles and standards of practice are governed by a complex set of nor-

---

[1] *See* U.S. MARINE CORPS, PUB. NO. 1, WARFIGHTING 47, (1997) ("[A] vulnerability that, if exploited, will do the most significant damage to the enemy's ability to resist…").

[2] *See infra* Section II. C.

[3] *Id.*

[4] *See infra* Section II. A.

[5] GARRY KASPAROV, DEEP THINKING: WHERE MACHINE INTELLIGENCE ENDS AND HUMAN CREATIVITY BEGINS 152 (Hachette Book Group 2017).

mative behavior and signed agreements reflected in the law of armed conflict and customary international law.[6] This article addresses the current disruption—a combination of artificial intelligence and machine learning as a means of executing quantum computing, using advanced algorithms, large data sets, and the underlying scientific principles of the universe for purposes of advanced decision making capacity and extraordinary computational power and speed—and its impact on the law of armed conflict principle of proportionality within cyberspace. Proportionality stands for the proposition that the goals of a strike and damage to civilians and civilian objects, must be balanced.[7] This technological iconoclasm may impact this principle, specifically, this disruption will have an impact on proportionality's nuanced mental assurance requirements for decision-makers which govern actions within a conflict—*jus in bellum*[8]—such as the permissible destructive results that follow those targeting decisions. This is an unfortunate circumstance as international law discourse is currently grappling with developing *en vogue* armed conflict rules and frameworks for application in cyberspace.[9] That discourse primarily focuses on what occurs on a strategic level.[10] The hypothetical demonstrates that this change in technology

---

[6] *See generally* NATIONAL SECURITY LAW DEPARTMENT, THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER & SCHOOL, U.S. ARMY, OPERATIONAL LAW HANDBOOK ch. 1-4 (Major Dustin Kouba et al. eds., 2018).

[7] *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Ship-wrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; [hereinafter Geneva Conventions]. *See also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) arts. 51(5)(b), 57(2)(a), 57(2)(b), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol].

[8] *See* DEP'T OF DEFENSE, LAW OF WAR MANUAL, ¶¶ 1.11 (2016) [hereinafter DOD LAW OF WAR MAN.]. (Providing that *Jus in bellum* concerns the law during the conduct of war while the *Jus ad Bellum* concerns the rules of resorting to force or going to war).

[9] *See generally* TALLINN MAN. ON THE INT'L LAW APPLICABLE TO CYBER WARFARE, 1.0 (Michael N. Schmitt, ed., Cambridge Univ. Press 2013); TALLINN MAN. 2.0 ON THE INT'L LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed., Cambridge Univ. Press 2017).

[10] *See generally* HERBERT LIN & AMY ZEGART., BYTES, BOMBS, AND SPIES: THE STRATEGIC DIMENSIONS OF OFFENSIVE CYBER OPERATIONS (Brooking Inst. Press 2018).

will cause decisions made at a tactical level of an armed conflict quickly make their presence known to strategic level considerations.[11]

The rules of *jus in bellum*—in short—generally hold that targets may be acquired and destroyed if criteria built from a "puzzle formed by hundreds of individual pieces of international law [agreements and customary practices by action] and domestic law" are met.[12] According to international sources such as *Hague Conventions of 1899* and *1907*, the *Geneva Conventions* after World War II and their *Additional Protocols* thereafter; international and domestic nation-court decisions; ancient customary law; U.S. domestic sources such as the *United States Code, Uniform Code of Military Justice*, federal agency regulation, case law, and military department field manuals; and even works from academia; a set of general targeting principles has been developed to conduct military targeting operations.[13] The interdependent principles of military necessity; distinction; proportionality; unnecessary suffering (humanity); and honor, [14]ensure that decisions and actions executed in warfare are conducted on a battlefield in a relatively humane and legally sufficient manner.[15]

This article deals mainly with Proportionality. This principle ensures legitimacy to conduct hostilities, as well as trust and confidence between nations that each will follow signed agreements and normative behavior by requiring decision-makers to go through a process balancing incidental civilian casualties and damage to infrastructure and the military advantage to

---

[11] In military nomenclature, there are usually three levels of war (sometimes four). These levels are war are: strategic, operational or campaign, and tactical. The Strategic level which focus activities directly on national policy objectives (not to be confused with 'national strategy' which uses all elements of a national power to obtain objectives). The Operational or Campaign level which links these national policy objectives to the tactical level by deciding where, when, and under what conditions to conduct armed conflict. The Tactical level focuses on particular missions that accomplish combat objectives which should lead to operational and strategic success. *See* U.S MARINE CORPS, *supra* note 1, at 26-32.

[12] Maj. Aaron L. Jackson and Colonel Kristine D. Kuenzli, *Something To Believe In: Aligning The Principle Of Honor With The Modern Battlefield*, 6 Nat'l Sec. L.J. 35, 41 (2018) ("[LOAC] is not a singular work of art, but rather, a puzzle formed by hundreds of individual pieces of international and domestic law.").

[13] *Id.*

[14] *See e.g.* DOD LAW OF WAR MAN., *supra* note 8, at ¶¶ 2.1-2.6.3.2; *See also* KASPAROV, *supra* Note 5, at Ch. II. Both sources cite a variety of references, cases, and treaties. This author has chosen to use these particular references as sources of U.S. interpretation of these general principles. The author believes that these sources capture the principles in a manner conducive to this article's discussion. Other sources, including those of allied parties such as the United Kingdom, Australia, and Canada may differ. That discussion is beyond the scope of this article.

[15] *See id.* at ¶ 1.3.4.

be achieved.[16] The U.S. has codified this principle as a matter of policy within its *Department of Defense Law of War Manual* (*DoD Manual*) which frames U.S. interpretations of the international law of armed conflict.[17]

Questions are raised as to the point in which these advanced technologies—AI, ML, and QC—are implemented on the battlefield cross the line of legal departure from that which is consistent with the above principle. Considering the technological sophistication involved with QC, AI, and ML, can the current standard be met by decision-makers if there is no true understanding of the technology, and how and why it chooses to make its decisions? Considering many countries do not and cannot bifurcate their communications or cyber networks from that of civilian infrastructure, how do we preclude asymmetric impacts on the civilian population for an elongated period of time? Are there limitations that can be put into place to check the decision-making process where an artificial intelligence agent using machine learning methodologies carries with it the power of QC? Are new rules required given the technological iconoclasms present, or has a new rule already emerged from past-practice and legal interpretation? Although these are complicated questions, if appropriate interpretation and recommendations can be developed, these impacts may be minimized, and answers may be developed to provide clarity to the situation. Thus, allowing use of advanced technologies such as QC in warfare in a responsible and acceptable manner.

This article seeks to analyze the impact QC will have on Proportionality. First, the discussion will focus on QC, AI, and ML typology, development trends, technical impacts, and targeting within the cyber domain. Second, the article will discuss the rule of proportionality, in general, as well as doctrinal interpretations and academic comment. Next, it provides real-world examples of proportionality's application in armed conflict. Third, the article will apply the principle to the introductory hypothetical. Lastly, the article will provide normative recommendations and concluding remarks. The aim of this article is, hopefully, to encourage further analysis, discussion, and development of legal academia regarding this increasingly important and complex technology and its relation to national security law and the law of armed conflict.

---

[16] *See* Geneva Conventions, *supra* note 7.

[17] DOD LAW OF WAR MAN., *supra* note 8, at ¶¶ 2.4.

II. Quantum Computing, AI and ML: typology, development trends, impacts on national security, and the "Black Box"

In short, quantum and its mechanics—which provide the foundation of QC—is about "information, probabilities, and observables, and how they relate to each other."[18] The properties, designs, and potentials of QC that accomplish this relationship will ultimately lead to the development of platforms capable of vast computing power and speed, and the rethinking of security measures used to protect information and other traditional military applications. AI and ML execute QC capabilities through the ability to mimic human critical thinking and complex decision making by training on massive data sets.[19] This facilitates the creation of algorithms to better tackle complex problem sets, giving a computing system the ability to learn from its experience and improve performance.[20] In turn, these impacts will force a reevaluation of the rules that govern targeting in warfare.

A. Typology

1. Quantum Computing

Quantum computing (QC) is the process by which computers use principles of quantum physics, mechanics, and information science for increased computational power and speed.[21] Quantum physics, mechanics, and information science, allow computers to perform simultaneous calculations by measuring the physical photons, electrons, or atom nuclei of data.[22] This is possible due to the continuous physical nature of photons that can contain values that exists in more than one state at once, making contributions in both states for computational power and speed.[23] Their existence in multiple states, and contributions to different but simultaneous calculations to

---

[18] SCOTT AARONSON, QUANTUM COMPUTING SINCE DEMOCRITUS 110 (Cambridge Univ. Press 2013) ("From [my] perspective, [quantum mechanics] it's about information and probabilities and observables, and how they relate to each other. [It] is what you would inevitably come up with if you started with probability theory, and then said, let's try to generalize it so that the numbers we used to call 'probabilities' can be negative numbers.").

[19] *See infra* Section II. C.

[20] *Id.*

[21] *See* EXEC. OFFICE OF THE PRESIDENT, NAT'L SCI. AND TECH. COUNCIL, ADVANCING QUANTUM INFORMATION SCIENCE: NATIONAL CHALLENGES AND OPPORTUNITIES (2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf.; *see also* Dr. Arthur Herman & Idalia Friedson, *Quantum Computing: How to Address the National Security Risk*, HUDSON INST. at Aug. 2018, at 2-9.

[22] Herman & Friedson, *supra* note 21, at 5; *see* Nayef Al-Rodhan, *Quantum Computing and Global Security*, GLOBAL POL'Y J., (2015).

[23] *See* Herman & Friedson, *supra* note 21.

accomplish a collective goal, are real examples of the utility of science-fiction theories that attempt to prove parallel existence, in reference to Dr. Manhattan's quote above. [24]

Quantum computing accomplishes this feat through the use of information known as *qubits*.[25] Qubits encapsulate the existence of data in more than one state through information science methodologies.[26] In classical computing, information exists in individual electronic signals or voltages known a *bits*; these bits can only carry values of zero or one (0, 1), but not both.[27] This forces classical computers to use algorithms for computing in the bits limited binary state.[28] Because qubits are physical in nature, its existence and properties are continuous. It can be harnessed in a two-dimensional form known as *superposition*, where information exists in multiple states at once through a process in which these superimposed qubits are intimately correlated and connected (even over a certain distance), known as *entanglement*; or, measured by process of noise known as *squeezing*.[29]

The physical nature of each photon and the harnessing and measurement of its continuous state reveals qubits as probabilities which distribute value at the time it is measured.[30] Thus, in theory, these qubits carry an infinite number of values of these "zeros and ones" or combinations thereof at all times until each measurement is conducted (0, 1, [00], [01], [10]...etc.).[31] As this methodology and process of harnessing and measuring information is perfected, encoding of information in those qubits occurs; and the serious implications of surpassing and replacing classical computing which uses binary states is evident.

2. Impacts and Implications on Computing Speed and Computation Power

Quantum computing's largest impact—in terms of weaponeering and warfare—will be its difference from classical computing speed and encryption scheme power. Classical computing

---

[24] *See, e.g.,* AMIT HAGAR, QUANTUM COMPUTING § 4.1.1 (Stanford Encyclopedia of Phil. rev. ed. 2019), http://plato.stanford.edu/entries/qt-quantcomp/.

[25] *See* Herman & Friedson, *supra* note 21.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.* at § 2; *see also infra* APPENDIX I of this article for more information.

[30] Herman & Friedson, *supra* note 21, at §§ 1 and 2.

[31] *Id.*

uses binary states of logic of "ones and zeros" to create linear coding.[32] In terms of speed, classical computing processing power involves a concept called "Moore's law," which postulated that processor speed and overall processing power for computers would double every one and one-half years.[33] This has driven development of computer chip fabrications that hold the transistors which allow *bits* of those "ones and zeros" to operate to become smaller and more powerful for economic-demand and hardware reasons.[34] Current levels of classical computing speed may have reached a plateau in keeping up with this demand, due to the inability to make chips smaller than current levels that can carry the processing power and speed needed, thus encouraging a search for faster and more powerful computing processes.[35]

Quantum computing changes this because of its ability to factor all possibilities of its existing state simultaneously, at once.[36] As opposed to only stringing together binary states of logic of "ones and zeros," the above discussed states of *superposition* and *entanglement* allow multiple strings of logic at once and in multiples of current binary code by a factor of two-times the *qubit*.[37] This means that current computing speeds will significantly surpass conventional computing methods due to sheer performance of binary operation.

In terms of encryption schemes that protect computing information, currently the best classical computing uses large mathematical operations known as *public-key cryptology* that demands access split between parties to unlock information hidden within the data.[38] Security protocols of large integers are used to scramble information as unreadable until this large string of integers is solved.[39] This is an asymmetric two-staged process by which one party generates a private key to decrypt information that can only be unlocked by a public key containing the answer to the integer.[40] The answer is generally available to a trusted party who is authorized to

---

[32] *See* Al- Rodhan, *supra* note 22.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *See id.; see also* Herman & Friedson, *supra* note 21, at 5.

[37] *See* KEITH CRANE, ET AL., ASSESSMENT OF THE FUTURE ECONOMIC IMPACT OF QUANTUM INFORMATION SCIENCE 43-44 (IDA Science & Tech. Inst. 2017) [hereinafter Crane, et al.].

[38] *Id.* at 33-34; *see also* Herman & Friedson, *supra* note 21, at 4-6.

[39] Crane, et al., *supra* note 37, at 33-34.

[40] *Id.*

unlock the problem.[41] This process is reliable because even with the fastest available conventional computing power attempting to forcibly break this encryption method by factoring the integer, it could take years—which is an unreasonable time period if one is attempting to intercept communication during, for example, a current military operation in need of the information contained within the data.[42]

Quantum computing's increased power due to *qubits* contains the ability to dramatically reduce the time needed to factor the integers of current encryption, thus rendering moot conventional security protocols for protecting information.[43] Quantum computing would be able to potentially find the solution to the integer by simultaneously generating answers for every possible scenario, as well as their alternatives at increasing speed.[44] From the description of QC, it is easy to see how current computing power and encryption schemes which rely on classical computing will be impacted.

3. New Approaches to Computing and Security

The impacts of QC will change the way in which computing power and encryption methodologies are implemented. Because of the vast power and speed QC will bring to the table, current computing methods and encryption methodology will implement QC. QC will offer more state's space to store information and better encryption schemes.[45]

As to computational power, Peter Shor's discovery of the algorithm which can factor large numbers by using quantum mechanics to perform faster calculations exceeding classical methods, and the subsequent demonstration by AT & T labs that it can actually perform first order logic operations, has led to effort to develop quantum computers that can someday replace classical computers.[46] It is currently understood that quantum phenomena can be harnessed in *qubits* to perform computing operations. The blending with information science—which allows efficient encoding and transmission of information— ultimately renders development of these

---

[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 21, at 2.

computers all the more real.[47] Massively complex calculations performed at increasingly fast rates will produce faster and more powerful computers for private, commercial, or public-military use that will lead to new computing power, dubbed "Quantum Supremacy."[48] Quantum Supremacy is where a quantum computer surpasses a classical one for general computing purposes by solving problems no classical computers can solve.[49] Many companies and nation-states are in a race to develop these computers, which will be discussed further below.[50]

In the 2018 report, *Quantum Computing: How to Address the National Security Risk*, Dr. Arthur Herman and Idalia Friedson list a number of primary systems to illustrate real applications of quantum computing technology.[51] Two of these systems are applicable for purposes of this discussion: (1) quantum annealers and (2) quantum computers.[52] The first type of computing involves a quantum annealer. Annealers are used to solve a multitude of optimization problems by performing calculations that do not disturb the states of *qubits*.[53] This machine takes samples and measurements to measure the natural tendency of the energy represented—including that of the *qubits* as they compute.[54] Certain types of metals are currently being used to implement this process and companies such as D-Wave Systems Inc. assert breakthroughs of using "thousands" of *qubits* for purposes of pattern recognition detection software used by machine learning tools, image analysis, and cyber security.[55]

---

[47] *Id.*

[48] *See* Herman & Friedson, *supra* note 21, at 4-8; *see also* Crane, et. al., *supra* note 37, at 33-34, 43-44.

[49] *See* Herman & Friedson, *supra* note 21, at 7.

[50] *See id.* at 13-19; *see also*, *e.g.*, Patricia M. Figliola, *Quantum Information Science: Applications, Global Research and Development, and Policy Considerations*, CONG. RES. SER. No. R45409, 1-3 (2018).

[51] Herman & Friedson, *supra* note 21, at 8.

[52] *Id.*

[53] *Id.*; *see also* Al-Rodhan, *supra* note 22, at 2.

[54] Al-Rodhan, *supra* note 22, at 2.

[55] *Id.*; *see also* Dr. Steve Adachi, *Near-Term Applications of Quantum Annealing*, Int'l Workshop on Quantum Annealing and its Applications in Science and Science and Industry (QuAASI), (Jul. 27, 2016), http://www.fz-juelich.de/ias/jsc/EN/Expertise/Workshops/Conferences/QUAASI16/Programme/Talks/quaasi16-adachi.pdf?__blob=publicationFile. "D-Wave's quantum computer leverages quantum dynamics to accelerate and enable new methods for solving discrete optimization, sampling, material science, and machine learning problems. It uses a process called quantum annealing that harnesses the natural tendency of real-world quantum systems to find low-energy states. If an optimization problem is analogous to a landscape of peaks and valleys, each coordinate represents a possible solution and its elevation represents its energy. The best solution is that with the lowest energy corresponding to the lowest point in the deepest valley in the landscape." D-WAVE SYSTEMS, *About Us*, https://www.d-wavesys.com/our-company/meet-d-wave (last visited Dec. 26, 2019).

The second system is a quantum computer.[56] This system requires the entanglement of *qubits* in a superimposed state to transmit information contained in data faster than conventional computers.[57] Again, this occurs by computing algorithms that no conventional computer could compute or by computing current algorithms faster than the best current super computers.[58] Currently companies such as Google, IBM, Microsoft, and China's Alibaba, have devoted resources to developing scalable quantum computers and had minimal success at quantum computation that transmits information held in *qubits*.[59] This will have real-world applications in every domain in which computers are currently operated. Progress is slow, however, as this computing method requires semiconductor chip circuits that can quickly overheat during the process. Current research focuses on cooling methods for this process or alternative methods for continued development of quantum computers.[60]

Specific applications in terms of national security and warfare involve radar, sensing, GPS, and encryption security.[61] In short, sensing will assist in protecting information by 'sensing' the disturbance of protected data's physical state. This is quite different from factoring its security protocol integer or detecting stealthy military hardware that disturbs *qubits entangled* states, using GPS to exploit more accurate measurements photons, and encryption by using more power factorization of integer security protocols. Using this methodology will create better security for its own quantum computing systems.[62] This is why nation-states as well as private industry is keenly focused on the development of this technology.

---

56 *See* Herman & Friedson, *supra* note 21, at 8.

57 *See* EXEC. OFFICE OF THE PRESIDENT, s*upra* note 21, at 6.

58 *Id.*

59 *Id.*; *see also* Elsa B. Kania & John K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, CENTER FOR A NEW AMERICAN SECURITY ¶¶ 3-5, (Sept. 2018), https://www.cnas.org/publications/reports/quantum-hegemony (last visited January 3, 2019).

60 Kania & Costello, *supra* note 59, at 4; *See also* Herman & Friedson, *supra* note 21, at 8.

61 *See* EXEC. OFFICE OF THE PRESIDENT, s*upra* note 21, at 4-7; Herman & Friedson, *supra* note 21, at 4-14; *see also* Kania & Costello, *supra* note 59, at 4-26.

62 Herman & Friedson, *supra* note 21, at 11, 13. Specifically, for security purposes, QC could use quantum random-number generators (QRNG) for truly random encryption keys based upon naturally occurring cosmic energy measurements; post-quantum cryptography using quantum resistant algorithms (QRAs) by using difficult mathematical equations and large[r] integers than those currently used by classical computers; and quantum communication networks based on the physical state of individual particles held in *qubits*.

B. Development Trends

In terms of industry and national security strategy, this disruption has garnered the attention of the U.S. government. A string of commissioned studies, orders, and policy assessments regarding this issue have recently surfaced.[63] For example, former President Barack Obama signed *Executive Order 13702*[64] in 2015, which provides that the U.S. government will "maximize the benefits of high-performance computing research, development, and deployment"—now known as a derivative of quantum computing (QC).[65] Moreover, the National Science and Technology Council produced a joint report which detailed the impacts of QC will have on certain fields of science such as high-performing computing, sensing, meteorology, and simulation.[66] It further states that the government must take a "coherent, all of government approach" to sustain and developing technology based upon Quantum Information Science (QIS) to manage its impact on these fields of study.[67] Lastly, the Government Accountability Office has issued a report on U.S. federal agency support of scientific and technological innovation that stems from enhanced technology such as quantum mechanics and quantum computing.[68] The GAO report, *Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research*, details current Department of Defense initiatives, ultimately concluding that federal agencies should take a "strategic approach" to support QC by creating interagency groups and define roles and responsibilities to accomplish common outcomes. This would ensure agencies maintain U.S. competitiveness and dominance in innovative technologies.

Other countries are also quickly developing QC and QIS capabilities.[69] China, the United Kingdom, Canada, and the European Union have all committed research and development in-

---

63 *See*, *e.g.*, Figliola, *supra* note 50.

64 Exec. Order No. 13,702, 80 Fed. Reg. 46,177 (July 29, 2015).

65 *Id.*

66 *See generally* EXEC. OFFICE OF THE PRESIDENT, s*upra* note 21.

67 *Id.* at 1.

68 *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-656, CONSIDERATIONS FOR MAINTAINING U.S. COMPETITIVENESS IN QUANTUM COMPUTING, SYNTHETIC BIOLOGY, AND OTHER POTENTIALLY TRANSFORMATIONAL RESEARCH AREAS (Sept. 2018), https://www.gao.gov/assets/700/694748.pdf.

69 *Id.* at 1 ("The United States is considered a world leader in many sciences and technology areas, but other countries, such as China, are also making increased investments in research [for quantum computing and quantum information science]. Increased competition from these countries has led some experts and others to express concern…").

vestments to explore this technology and its real-world applications.[70] Out of these countries, China appears to be the leader and main competitor of the U.S., especially in its development of QC and QIS capabilities in combination with artificial intelligence and machine learning for military applications.[71] This demonstrates an international "arms race" for the next advanced military capability to gain an edge on the battlefield that moots competitors' current technological capabilities.

C. Artificial Intelligence, Machine Learning, and the Impact on National Security and Armed Conflict

The current technology which makes QC and QIS so dangerous would be their combination with artificial intelligence and machine learning. Artificial intelligence can be generally defined as a computer science program's ability to solve complex problems through a process that mimics human critical thinking; it must be able to receive information, critically analyze information, act on such information, and store that decision-making process for future application.[72] Machine learning adds another layer of intelligence to artificial intelligence by allowing it to train on massive pre-programmed data sets that are matched via algorithms through a variety of methods such as adversarial competition, micromanagement, and other corrective measures.[73] Machine learning enables predictive models that may serve artificial intelligence in making rational decisions in a variety of environments.[74] This ability to "think" and act critically in a given situation, as well as the ability to improve such behavior through programming and experience, make applications of QC and QIS all the more pressing for military powers.

From a national security and armed conflict standpoint, QC and QIS may give certain countries strategic advantages in intelligence and warfighting. Combined with artificial intelli-

---

[70] *Id.*

[71] *Id.*; *see also* Kania & Costello, *supra* note 59.

[72] *See* Salahudin Ali, *Cybersecurity Support of Insider Threat Operations: DoD Regulation and Constitutional Compliance*, 30 GEO. MASON U. C.R.L.J. (forthcoming 2019*)*; *see also* Appendix II of this article for more information.

[73] Ali, *Cybersecurity Support of Insider Threat Operations*, *supra* note 72; *see also* APPENDIX III of this article for more information.

[74] *Id*.

gence and machine learning capabilities, this advantage has been called *battlefield singularity.*[75] Battlefield singularity connotes the concept that artificial intelligence will surpass human decision-making capability and weaponize available information to analyze and act faster than an opponent during conflict to achieve a decisive decision on the battlefield.[76] This could involve syncing commanders, their platforms such as unmanned aerial vehicles, and their artificial intelligence tools that use machine learning for a coordinated operation on a traditional battlefield. In an intelligence environment, this could involve the deciphering of sensitive communications that are ongoing or stored, or the detection of infiltration of adversary eavesdropping attempts with ease. This would allow advanced situational awareness of adversary action and intentions. Essentially, the mass accumulation of data and ability to analyze and learn from the data, and the push of analytics to tools and platforms in the battlefield puts an adversary at a critical disadvantage.

This singularity combined with the potentially massive computing power QC brings to the table changes the dynamic by given a competitive edge on the battlefield. However, without effective control or insight into the these tools decision-making processes, that advantage could become a liability in regards to what the competitive edge is supposed to achieve in a conflict.

D. The "Black Box"

The issue that may arise from this singularity of combined QC, AI and ML, is an understanding of how and why a platform that uses them makes decisions. This is known in AI nomenclature as "Black Box" AI.[77] "Black Box" AI is generally considered "the inability to fully understand an AI's decision-making process and an inability to predict the AI's decisions or outputs."[78] It can be classified as strong or weak—"strong" being a complete inability figure out

---

[75] *See* Elsa Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, CENTER FOR A NEW AMERICAN SECURITY (Nov. 28, 2017), https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.

[76] *Id.*

[77] *See* Yavar Bathaee, *The Artificial Intelligence Black Box And The Failure Of Intent And Causation,* 31 HARV. J. L. & TECH. 890, 905 (2018).

[78] *Id.* ("Generally, the [Black Box Problem] can be defined as an inability to fully understand an [AI's] decision-making process and the inability to predict the [AI's] decisions or outputs."). Outputs are those actions or decisions taken by the AI agent based on information perceived and experience. *See* STUART RUSSEL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 1-59 (3d ed. 2016).

why and how an AI does what it does, and "weak" being the ability to probe for some limited idea in the AI's decision-making process—but common to both is the opaqueness to humans.[79]

The function AI and ML tools used to perform are opaque because of the complexities involved in the algorithms. Countless artificial neurons, deep neural networks, and interconnectedness of networks, resemble and function like a human-brain that learns from experience.[80] The large data-sets and training methods produce a level of intuitiveness that pulls aggregate knowledge from individual neurons in large networks, each neuron performs the function of weighing and calculating individual forms of data to produced better algorithms.[81] These algorithms, in-turn, are used to produced better performance for a tool or platform's assigned goals.[82] To attempt to understand these complex layers and dimensions would be like trying to solve the secrets of neural science related to the human brain, an ongoing process. One would have to calculate and know why a certain weight is given to a gradient or piece of data as it travels through layers of neural networks.

Moreover, algorithms can also be used to seek and find hidden variables and pattern-recognition.[83] Methodologies include classifying types of behaviors, objects, and other data points by using separation points.[84] An AI platform uses ML algorithms to create these separations points to pick-out patterns, variables, and common characteristics of data.[85] Depending on what separation points are used to identify these patterns and variables, it can become impossible to figure out exactly which separation points are being used.[86] For example, a commander may program a platform or tool to identify enemy soldiers in a conflict zone. The platform or tool uses the data point of enemy flags attached to green camouflage to distinguish enemy soldiers from civilians in a conflict-zone. This is an easy observation to make, but would possibly be prone to too many anomalies—maybe green camouflage is a fashionable item in the said-named

---

79 *See* Bathaee, *supra* note 77, at 905-6.
80 *Id.* at 897-906.
81 *Id.*
82 *Id.*
83 *Id.*
84 *Id.* at 904 figs. 3 & 4.
85 *Id.* at 905.
86 *Id.*

country. The algorithm can be further refined to limit this data point to only those who also where camouflage blouses and trousers, and so on and so forth. Eventually the platform or tool will start to characterize and classify those it identifies as threats based on this criteria (of course with outliers) using separations points that are no longer observable (so far, those other than green camouflage, blouses, trousers, etc.) to humans.[87]

This situation is exacerbated with the addition of QC, any difficulty in attempts at understanding "Black Box" AI would be increased as increased speed and different foundations for algorithms—quantum information science and quantum mechanics—would be used. Understanding of this technology is vital to the standards and criteria provided by the law of armed conflict (LOAC) principle of proportionality, because that analysis requires a certain level of knowledge regarding expected casualties and damage, as well as how a decision contributes to the military mission.[88] If a commander is unable to predict the results of her actions nor understand why her weapon system makes decisions, she may not be able to form the requisite level of mental assurance to conduct an attack.[89]

III. Cyberspace Domain and Targeting

The tools of QC, artificial intelligence, and machine learning will be used in and through cyberspace. There are various definitions of cyberspace, but the DoD defines it as "[a] global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[90] This domain is trifurcated into layers which consist of the physical layer, the logical layer, and the cyber-persona layer.[91] Each layer is distinct upon its characteristics but related into how they interact with each

---

87 *Id.*

88 *See* Additional Protocol, *supra* note 7, at art. 51(5)(b).

89 *Id.*

90 JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS, at GL-4 (June 2018) [hereinafter *JOINT PUB. 3-12*]; *see also* William Gibson, *Neuromancer* (1989) (containing one of the first ever definitions of cyberspace, although it is science-fiction) ("A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data."); *see also* Richard A. Clarke & Robert K. Knake, *The Cyber War: The Next Threat to National Security and What to Do About It* (2010) ("Cyberspace is all of the computer networks in the world and everything they connect and control."). What can be gathered from these myriad of definitions is that cyberspace involves computers/devices, networks that connect them, and users of such computers/devices and networks.

91 JOINT PUB. 3-12, *supra* note 90, at I-2 to I-5.

other in use. The physical layer represents devices and infrastructure that is represented in hardware such as storage components, computers frames, or data centers.[92] The logical layer consists of networks and software that related to another, which is represented by IP addresses, codes, websites script, or metadata.[93] The cyber-persona layer represents the abstraction of data that describes users or uses of the logical layer; this could be individual users, automated systems, or organizational accounts.[94] All three layers will be impacted by QC, many nations conduct cyberspace operations as a means of warfare, including the Department of Defense (DoD).[95]

Within these layers lay important entities, objects, and gatherings of people (networks in the cyber-persona layer) that if impacted or destroyed, contribute to a military mission. These are known as targets; a target is considered an entity or object that functionally operates as a threat for engagement or other action. [96] Targeting is the process of "selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities."[97] Determining and prioritizing targets requires a cyclical process of nominating, prioritizing, developing (through intelligence and preparatory actions) and deciding on which targets to engage, employing appropriate capabilities to accomplish a mission's intent on the target, assigning forces to accomplish the task, and assessing the impact of such targeting.[98] This cyclical process begins and ends with the commander's intent and desired effects she seeks as an outcome that contributes to her overall mission, tying her actions to that of the overall military campaign.[99]

In cyberspace, this is conducted by using a process of accessing, enumerating, prioritizing, and taking action that exploits some vulnerability of one or all three layers of a cyberspace

---

92 *Id.* at I-3.

93 *Id.* at I-4.

94 *Id.*

95 *See* DoD Law of War Man., *supra* note 8 at 1012 ("Cyberspace may be understood to be those operations that involve the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.") (internal quotations omitted).

96 Joint Chiefs of Staff Pub. 3-60, DoD Dictionary Of Military and Associated Terms 231 (Feb. 2019).

97 *Id.* at 232.

98 Maj Steven J. Smart, *Joint Targeting in Cyberspace*, AIR & SPACE POWER J., 69-70 (2011) (The author pulls his analysis from JP 3-60, but this publication is unavailable to the public); *see also* Joint Targeting School, Joint Targeting School Student Guide (2017), https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067 (last visited, Mar. 28, 2019).

99 *Id.*

target—this most likely occurs within the larger steps of development and capabilities matching during a traditional targeting cycle analysis.[100] Accessing includes the ability to take advantage of a system and deliver a desired effect; enumerating includes the process of mapping and identifying key aspects of a system; prioritizing includes a command decision of ranking which targets will best achieve a mission's intent; and exploiting includes the process of delivering impacts—through payloads such as malware, etc.—to the system that achieve a mission's intent.[101] Targeting is conducted based upon relevancy in achieving a commander's objectives overall, not for the sake of availability.[102] Types of targeting may be classified as easy or difficult; and remote or close; regardless, a commander must weigh all of these considerations during a targeting process cycle.[103]

The assistance of QC, AI, and ML methodologies can quickly complicate an already nuanced process of targeting analysis. Factual issues of why a particular target is developed and why a certain effect has been chosen can be easily lost if decisions within this cycle are delegated or replaced by tools meant for assistance during this targeting process such as AI, ML, and QC. This may be a contribution of the aforementioned "Black Box" AI problem—the complex process of deep neural networks, algorithms, and optimization of pattern recognition—that make it hard for humans to visualize and understand how and why a AI tool using ML methodologies makes decision.[104] Although cyberspace brings with it these sets of differences from traditional targeting during an armed conflict, targeting must adhere to international law and DoD policy that govern targeting decision making process and development.[105] This means that regardless of

---

[100] JP 3-12, *supra* note 90, at IV-8 to -9; *see also* Salahudin Ali, *The Bloody Nose*: 10 U.S.C. § 395, 6 NAT'L SEC. L. J. 127 (2018) (forthcoming).

[101] JP 3-12, *supra* note 90, at IV-8 to -9; *see also* Smart, *supra* note 98, at 69-70. (The author pulls his analysis from JP 3-60, but the current version of JP 3-60 is unavailable to the public).

[102] JP 3-12, *supra* note 90, at IV- 9 ("The focus [of targeting] is on creating effects that accomplish targeting-related tasks and objectives, not on using a particular cyberspace capability simply because it is available.").

[103] *See* Ali, *The Bloody Nose*, *supra* note 100.

[104] Yavar Bathaee, *The Artificial Intelligence Black Box And The Failure Of Intent And Causation,* 31 HARV. J. L. & TECH. 890, 897-905 (2018) ("The complexity of these countless neurons and their interconnections makes it difficult, if not impossible, to determine precisely how decisions or predictions are being made. [A]lgorithms can also create a black-box problem because they process and optimize numerous variables at once by finding geometric patterns in higher-dimensional, mathematically defined spaces.").

[105] *See, e.g.*, DOD LAW OF WAR MAN., *supra* note 8, at 1013-1024; *see* JP-3-12, *supra* note 90, at IV-8; *see* Smart, *supra* note 98, at 66-67.

the tools used in cyberspace, there is no exception or exemption available that will permit targeting in this domain without looking to international law targeting principles to intelligently analyze the legality and impact of their uses. A failure to do so may result in a serious violation given the unknown inputs that are often associated with cyber domain targeting and advanced technologies.

IV. Impact on the Principle of Proportionality

The discussion above has thus far focused on typology, its relationship with current cyber targeting, its impact on the national security and intelligence landscape, and the means of delivery for QC capabilities. The legal principles of LOAC are how we view this impact and its legal implications during an armed conflict.

First, it is important to note what this analysis is not about avoiding confusion. First, it is not about whether it is legal to use QC or QIS in warfare altogether. That process is conducted in accordance with international law and U.S. policy to ensure a technology or weapon has the capability to distinguish between civilian and military objects, and does not cause superfluous injury or unnecessary suffering (in terms of pain to an individual actor) as designed.[106] Second, we are not concerned with a debate as to whether these principles are correct or are truly governing in a conflict—the U.S. has accepted these principles through signed agreement or as customary international law, and has mandated compliance with them through *Department of Defense Directive 2311.01E* .[107] Third, the remaining principles of military objective, distinction, and honor may be met due to nation-state communication systems being dual-use for military *and* civilian purposes.[108] Fourth, we are not concerned with whether an "armed conflict" truly exists or not. These principles apply to situations where parties intend to conduct kinetic hostilities or where parties are conducting kinetic hostilities; the existence of a shooting-war in our hypothetical would appear to meet this criterion.[109] Finally, for the sake of analysis, we are to assume an "at-

---

[106] Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Respecting the Laws And Customs of War on Land, art. 23(e), Oct. 18, 1907, 32 Stat. 1803, 1 Bevans 247 [hereinafter *Hague Convention (IV)*] ("[It] is especially forbidden [to] employ arms, projectiles, or material calculated to cause unnecessary suffering.").

[107] *See, e.g.*, DEP'T OF DEFENSE, DIRECTIVE ON DOD LAW OF WAR PROGRAM No. 2311.01E ¶¶ 4-5 (2011).

[108] *See, e.g.*, DOD LAW OF WAR MAN., *supra* note 8, at §§ 5.6.1.2.

[109] *Id.* at § 3.4.

tack" has occurred which qualifies the use of LOAC principle analysis due to the physical damage the system has suffered due to the attack—the absence of an attack means that no targeting analysis needs be completed.[110] Here, we are concerned with its effects on targets once used, and how it affects decision-making under an existing acceptable legal regime. The accepted interdependent principle this article is concerned with is Proportionality. This principle ensures the impacts of warfare through target selection are limited and are conducted in a manner acceptable to the international community.[111]

Proportionality has been adopted by the international community as customary law and by acceptance through signed agreements.[112] The general principle found in *U.N. Geneva Convention, Article 51* of *Additional Protocol I* (*1977*) is the controlling document for signature parties.[113] The U.S. has adopted this principle in its *DoD Manual* as a matter of policy to facilitate consistency in legal interpretation and to "address the law that is applicable to the [U.S.]."[114] Originally published in 2015 and updated in 2016, the *DoD Manual* serves as official U.S. interpretation of international law but cautions that it does not serve as a "substitute for the careful practice of law."[115] This means that—although a guide for interpretation of international law—each instance during an armed conflict must analyze LOAC principles dependent upon a specific circumstance, as opposed to using the *DoD Manual* as a broad brush to reach an intended conclusion.

As with any practice of law, the general legal rule serves only as a starting point. Interpretations are elastic and new rules can and must be created to carry-on with the times. In this

---

[110] Col. Gary Brown, USAF (Ret.) and Maj. Isreal King, USAF, *An Airman's Guide to Cyber Power: Cyberlaw and Policy*, AIR UNIVERSITY (Jul. 6, 2017), https://www.airuniversity.af.edu/CyberCollege/Portal/Article/Article/1238536/cyberlaw-and-policy/; *see* TALLINN MAN. 2.0 ON THE INT'L LAW APPLICABLE TO CYBER WARFARE, *supra* note 9, at 106-07 (There must be an "attack" to warrant LOAC analysis, if not, then the principles do not apply. A current standard is a test developed by Prof. Michael N. Schmitt, where he describes an attack in the sense of *jus in bellum* as having a tendency to result in damage or destruction to objects or injury or death to people).

[111] *See* Geneva Conventions*, supra* note 7.

[112] *Id.*

[113] *Id.*

[114] DOD LAW OF WAR MAN., *supra* note 8, at 1 ("This [manual] seeks to address the law of war that is *applicable* to the United States, including treaties to which the United States is a Party, and applicable customary international law.") (emphasis added); *see also* DEP'T OF DEFENSE, supra note 107, at ¶ 5.1.3.

[115] *Id.*

new, murky world of QC, AI, and ML, interpretation of international law may present interpretations consistent with established legal policy.

A. The Principle of Proportionality

The principle of proportionality is defined by the limitations it places on the incidental but expected damage to property, loss of life, and injury to civilian populations caught between the conduct of hostilities.[116] It generally holds that these incidental results of targeting must be reasonable and cannot be "excessive" in relation to the direct and concrete military advantage gained by striking a target—even if the action is justified, the relevant language provides that it is prohibited to conduct:

> [A]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[117]

Moreover, this rule is repeated in *Article 57 (b)* of *Additional Protocol I*:

> [A]n attack shall be *cancelled* or suspended if it becomes apparent that…attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[118]

This principle requires unpacking as many of its terms are vague and left to subjective judgement. The relevant elements from this principle are: 1. there must be an attack; 2. civilian loss of life, injury, or damage to civilian objects, or a combination thereof is expected; 3. there is a concrete military advantage anticipated for the action; 4. the expected civilian loss of life, injury, damage to civilian objects, or a combination thereof, is excessive compared to such concrete and direct military advantage. If elements one, two, and four are met, the attack must be cancelled or suspended, likewise if just element three fails, the attack must also be cancelled.[119] It is important to note that this process of unpacking is significant; this is highlighted by cyber

---

[116] Additional Protocol, *supra* note 7, at art. 51(5)(b); *see also* DEP'T OF DEFENSE, *supra* note 107, at ¶ 4-5; *see also* DOD LAW OF WAR MAN., *supra* note 8, at 60.

[117] Additional Protocol, *supra* note 7, at art. 51(5)(b).

[118] *Id.* at art. 57(2)(b).

[119] *Id.* at art. 51(5)(b).

operations scholar and practitioner Commander Peter Pascucci, United States Navy, JAGC, where he states, "[u]nderscoring the importance of the proportionality analysis, *Article 57 (2) (a) (iii)* repeats [for a third time] the standard and precludes those planning, launching or executing attacks from proceeding with the attack if it becomes apparent that the attack would violate the principle."[120]

An attack is evident when kinetic actions result in some form of damage, destruction, injury, or death (for purposes of this article, we assume both parties are in an open armed conflict and have inflicted kinetic impacts on each other), the hypothetical above indicates at least some form of damage is expected on the physical layer of a communication network.[121] Likewise, the hypothetical demonstrates that the military advantage to be achieved is to stop the adversary-party's ability to effectively command and control its forces; thus a concrete objective exists.[122] Thus points one and three are satisfied. However, points two and four become murky when applied to the hypothetical.

Attacks aren't expected to avoid loss of life, damage, or injury to civilians and civilian infrastructure altogether, but they must not be excessive or unreasonable.[123] Excessiveness and reasonableness are not defined in international law, but may be defined by the level of directness and concreteness of a targeting action.[124] Thus, a subjective balancing test, based upon available battlefield data which estimates physical damage, potential civilian casualties, and risk to sensitive infrastructure, drives the decision-making process of a commander wishing to execute a targeted strike.[125] In other words, the commander must be reasonably well-informed under the circumstances based on the information available to her that excessive civilian casualties and dam-

---

[120] *See* Peter Pascucci, CDR, US Navy, JAGC, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINN. J. INT'L L. 419, 445 (2017).

[121] DOD LAW OF WAR MAN., *supra* note 8, at ¶ 3.4.

[122] *See supra* Section I. A.

[123] DOD LAW OF WAR MAN., *supra* note 8, at § 2.4. n. 67.

[124] *Id.*

[125] *Id.*

age will not result from her action.[126] Due to this subjective burden placed on commanders to determine whether a particular military action results unreasonable or excessive damage, commanders maintain the responsibility to accurately assess such information available to them, as well as always act in good-faith based on such information.[127] This information is available through collateral damage estimates, battlefield intelligence, and other information gathering methods.

Reasonableness may be shown if the commander can explain—based upon an assessment of such information—the importance of a target and how it contributes to the overall mission and that the incidental damage is not expected to outweigh such advantage.[128] Thus, the burden may be overcome as long as feasible precautions are taken during the planning and targeting analysis cycle of a strike to limit harms to civilians and those not involved in an example, a commander may determine time, location, and weaponeering to accomplish this task and comply with this principle.[129]

This is not to say that a decision to strike must be perfect one, if a "military advantage"—those tactical gains that can also be linked to the overall armed conflict strategy—can be demonstrated, commanders will not be subject to second-guessing regarding their operational decisions where critics may benefit from Monday morning quarterbacking.[130] This is because "extensive" damage is not the standard, only "excessiveness."[131] Civilian use or civilian elements tied to a target will not exempt it from military action—true, this situation may produce a moral dilemma for the decision-maker given the fact that human life is measured against tactical and strategic

---

[126] GARY SOLIS, LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW 303 (2d. ed., Cambridge Univ. Press 2016) (quoting Prosecutor v. Galic, IT-98-29, ¶ 58 (2003)) ("In determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making use of the information available to him or her, could have expected excessive civilian casualties to result from the attack.")

[127] *Id.* at 195-96.

[128] *Id.* at 244-43. A note of caution is warranted here. Many commanders make the argument that "force protection" serves as part of the analysis. This may result in picking the most destructive, but inaccurate, method for an attack. Force protection is not part of the proportionally test, thus a commander cannot claim an expectation that excessive damage is not expected if they intentionally choose a means that promote such a prospect. *See* Solis, *supra* note 126, at 304-05; *see also*, Additional Protocol, *supra* note 7, at art. 51(5)(b).

[129] *See* NATIONAL SECURITY LAW DEPARTMENT, *supra* note 6, at 11. *See also infra* Section IV.

[130] *Id.*

[131] Additional Protocol, *supra* note 7, at art. 51(5)(b).

gains—but the proportionality rule is elastic enough to promote responsible decision-making in such a situation.[132] In other words, if a commander can foresee the contribution a successful strike may have on the conflict as a whole, she may choose to execute the strike in-light of the balancing test and harm estimates she conducts with her staff.[133]

This balancing test of proportionality is tricky when it comes to the cyberspace domain in which the commander seeks to use an AI, ML, and QC weapon platform. For instance, the line is not concisely drawn where the results of strike end, nor is it clear where the AI and ML platform that uses QC will draw the line of what it considers the commander's target as a military advantage based upon her balancing analysis. The task has been left to entity doctrine development and academia to find it.

B. Interpretation & Discourse

1. Doctrine

Attempts have been made to codify this balancing test to address the uncertainty in both the international law arena and the DoD as it relates to the cyberspace domain. The *Tallin Manual, Rule 113*—a publication produced by a group of international law experts and considered influential to international law—provides that "a cyber-attack that may be expected to cause incidental damage incidental to the loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is *prohibited.*"[134] This rule mirrors the principle of proportionality provided by Article 51 of *Additional Protocol I*, but addresses concerns that cyber-attacks may be conducted over civilian networks, which may cause excessive collateral damage to them. Collateral damage is defined as not only the initial impact, but also the second and third-order effects.[135]

---

[132] *See* Solis, *supra* note 126, at 295-305.

[133] TALLINN MAN. 2.0 ON THE INT'L LAW APPLICABLE TO CYBER WARFARE, *supra* note 9, at 474, 478 n. 1144 (providing an example of the *Galic* Judgement, stating: "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or here, could have expected excessive civilian casualties to result from the attack.").

[134] *See id.*, at Rule 113 (emphasis added).

[135] *Id*. (emphasis added); *See also* Additional Protocol, *supra* note 7, at art. 51(5)(b).

Like Article 51, the military advantage cannot be merely speculative, it must be reasonably foreseeable that it will contribute to the overall military campaign.[136] Reasonableness is judged by the analysis consisting of those first-order effects (direct consequences of a targeting action, unaltered by intervening events) and those second and third-ordered effects (consequences which are delayed, altered, or intervening due to the first-order effects).[137] For example, the use of a certain malicious software during an attack may be uncontainable, or—as demonstrated in this article's hypothetical—an AI and ML platform could make decision to execute an attack in ways not foreseen by a commander. Conducting this analysis shows the difference and difficulty as compared with a traditional analysis, because in a traditional sense, the second and third-order effects may be rare or clearly identified.

The DoD Manual attempts to address the issue of proportionality in cyberspace by first providing that the proportionality rule applies to cyberspace.[138] It stresses the importance of a commander analyzing the potential effects that are remotely removed from the targeting, as well as the "lesser forms of harm" such as inconveniences and disruptions to civilian network infrastructure.[139] The same feasible precautions and subjective balancing test in a traditional sense, are extended for purposes of cyber-attacks.[140] The DoD Manual appears to do the most work by what it does *not* consider excessive damage; that being, minor disruptions of services or internet services, brief disruption or interference with communications, or even defacing a webpage.[141] Thus, it is a helpful guide for application of proportionality for targeting in this domain.

Lastly, international organizations, such as the Shanghai Cooperation Organization, have put limitations on the use of cyber weapons employed in the cyber-persona domain (information operations) by providing that operations which "use information resources without relevant

---

136 Additional Protocol, *supra* note 7, at art. 51(5)(b).
137 *See* TALLINN MAN. 2.0 ON THE INT'L LAW APPLICABLE TO CYBER WARFARE, *supra* note 9, at 472.
138 DOD LAW OF WAR MAN., *supra* note 8, at 1022.
139 *Id.* at 1021.
140 *Id.*
141 *Id.* at 1022.

rights or in violations of the *existing rules and laws of states or norms of international law*[.]" [142] This is important given that key signatories (Russia, China, and other four former Soviet states) of this organization consider information operations, by definition, part of the overall cyber domain operating environment.[143] This captures a broad scope of activities that could possibly be interpreted as excessive (subject to cultural and political norms of the nation-state). One could infer the purpose of capturing broad scopes of cyber-persona activity is meant to quell political dissidents from these nation-states.[144] Whatever the case, this rule would mean that information operations as part of the cyber-persona layer of the cyber domain, are subject to the same requirements of proportionality.

2. Selected Academia

Attempts at defining the rule and applying it to the cyber domain have also been prevalent in academia.[145] Due to the terms used in the proportionality rule and the lack of doctrinal guidance, academic discourse has made attempts to define the terms, call attention to its application to the cyber domain and advanced technologies, and create workable standards and solutions for the rule's application.[146]

Professor Gary Solis, in his second edition of *Law of Armed Conflict: International Humanitarian Law,*[147] discusses the principle of proportionality—generally—and offers his insight. He notes that "excessiveness" is an unclear but elastic concept that is left to legal interpretation.[148] Violations, he provides, have to be "clearly" disproportionate to the military

---

[142] AGREEMENT BETWEEN THE GOVERNMENTS OF THE MEMBER STATES OF THE SHANGHAI COOPERATION ORGANIZATION ON COOPERATION IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY, 61ST PLENARY MEETING at 210 (Dec. 2, 2008) [hereinafter SHANGHAI COOPERATION AGREEMENT]; *see also* JOINT PUB. 3-12, *supra* note 90, at I-2 to I-5.

[143] SHANGHAI COOPERATION AGREEMENT, *supra* note 142, at 209 ("'Information war' [-] confrontation between two or more states in the information space aimed at damaging information systems, processes and resources…"). ("'Information infrastructure' [- array] of technical means and systems to generate, transform, transfer, use and store information [.]") ("'Information space' [-] field activities related to generating, transforming, transferring, using and storing information which influences….information infrastructure [.]").

[144] Hensey A. Fenton III, *Proportionality And Its Applicability In The Realm Of Cyber*-Attacks, 29 DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 335, 342 (2019).

[145] *See, e.g.*, Solis, *supra* note 126; Michael Schmitt, *Law of Cyber Warfare: Quo Vadis?* 25 STAN. L. & POL'Y REV. 264 (2014); *See also* Pascucci, *supra* note 120; *see also* Bathaee, *supra* note 104.

[146] *Id*.

[147] *See* Solis, *supra* note 126.

[148] *Id.* at 294.

object to be achieved; close calls don't count.[149] This may be due to the recognition by the rule's commentary that civilian objects that are verifiably used by military forces (*dual-use* rule) can be attacked.[150] In such instance, the proportionality rule kicks-in as customary law that cannot be ignored, requiring balancing of those potential civilian casualties and damages, methods used to attack such a target (access to intelligence estimates, battlefield information, and weaponeering), and a non-negligible decision that accepts unnecessary loss and damage.[151]

Professor Solis further explains that this proportionality analysis avoids actions that are "clearly" disproportionate and excessive by not merely engaging in an exercise of collateral damage estimates.[152] Indeed, collateral damage estimates have become somewhat of a trendy euphemism for proportionality analysis, which is incorrect.[153] Although useful for a proportionality analysis in providing data on expected civilian casualties and resources, the estimate does not do the work that proportionality analysis requires. Instead, pulling all available information and weighing it against the military mission's end-state is the requirement.[154] This requires good-faith efforts in looking at the data and a reasonable decision that does not intentionally aim to harm civilians, but one that an outside observer could see a targeting ends to the targeting's means.[155]

Professor Michael Schmitt in his article, *Law of Cyber Warfare: Quo Vadis?,*[156] provides that proportionality analysis depends on what an "object" or "damage" entails.[157] He goes on the to note that commentary—provided by the International Committee of the Red Cross—to the proportionality principle interprets "object" as something visible and tangible.[158] Data doesn't fit neatly into something that is visible and tangible, but it can be represented in electronic docu-

---

[149] *Id.* at 294-5.

[150] *Id.* (dual-use refers to an object that is used for civilian and military purposes.)

[151] *Id.* at 295 n. 160 (quoting Prosecutor v. Kupreskic and Others, IT-95-16-T (2000)).

[152] *Id.* at 294.

[153] *Id.* at 295.

[154] *Id.* at 303.

[155] *Id.* at 295.

[156] *See* Schmitt, *Law of Cyber Warfare, supra* note 145, at 297-99.

[157] *Id.*

[158] *Id.* at 297 ("The [ICR] commentary to the [Additional Protocols] describes an object as something that is 'visible and tangible.'") (emphasis omitted).

ments or storage formats.[159] For example, medical data represented by zeros and ones in computer coding are codified in electronic word documents that can be printed into something tangible and visible. If the electronic system is destroyed, so goes the potential tangible and visible representation. The commentary interprets "damage" to include diminishing significance of physical infrastructures that hold data.[160] This may be a judgement on the pre and post attack value of a target. Following this logic, an attack that excessively damages this data without a clear military objective may violate the principle.

This is not meant to promote overreach, as Professor Schmitt warns, many of these forms of damage are appropriately categorized as information operations and use the layers of the cyber domain as a means to an end; data can be manipulated, but not destroyed to achieve the military purpose.[161] Outside of attacks on a larger internet or other communication network that would excessive damage in the form of diminishing significance—partly due to the loss of functionality, it is doubtful that this view of "diminishing" value test would receive extensive consideration as a stringent rule.

Commander Pascucci, in his article, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real World Solution,*[162] concludes that clarity is needed from an international doctrine to provide guidance in facilitating assessment of direct and indirect effects an attack in cyberspace may have.[163] He also argues that—currently—data is not a pure object, it can be corrupted or manipulated, but that does not equate to destruction according to modern interpretation.[164] Only the underlying physical system is prone to destruction because attacks signify an "act of violence against an adversary."[165] But can this also include data? Does it include the loss of functionality? This question is best understood from the point of view that the

---

[159] *Id.*

[160] *Id.*

[161] *Id.*

[162] *See* Pascucci, *supra* note 120.

[163] *See id.* at 447-48 ("Determining which of [these] effects constitutes 'damage' for the purpose of [international humanitarian law] is a necessary predicate to ascertaining whether an injury or damage is excessive in relation to the direct and concrete military advantage anticipated.").

[164] *Id.* (Presently, a reasonable interpretation of international humanitarian law would cause a commander to select a cyber-attack that may result in collateral damage destroying terabytes of data…over a kinetic strike that is expected to result in…civilian casualties.").

[165] *Id.* at 442.

"knock-on" effects of a cyber-attack on information or an infrastructure can have "knock-off" effects that flow from them that need to be considered.[166] The primary concern being that those initial "knock-on" effects will have unexpected "knock-off" effects that were not intended.

Clarity in terms will assists with the *ex-ante* proportionality analysis of expected casualties and damage which will be subjected to *ex post facto* judgement regarding a commander's decision to attack a target in the cyber domain.[167] Indeed, the technology makes it difficult to develop a methodology for such an analysis. If clarity can be given to what "effects" constitute excessive damage, decision-makers can perform a proportionality analysis as they did before in a kinetic sense with a clear understanding of the expected damage and its potential excessiveness considering the direct and concrete military mission.[168]

In his other article, *Uncertainty in the Law of Targeting: Towards a Cognitive Framework*,[169] Professor Schmitt introduces a mental formulae that could potentially capture the analysis of effects, damages, and expectations thereof in terms of proportionality.[170] He introduces this framework not to replace the subjective judgment of commanders, but to promote a critical analysis that pushes decisions beyond being "certain enough" about the effects and military advantage a target might produce in the face of battlefield uncertainty and ambiguity.[171] The framework works in a mathematical expression by taking the value of each civilian or civilian object and the probability of collateral damage to each, eventually reflected in a total denoting sum of all collateral damage that needs to be considered.[172]

Professor Schmitt highlights a formula is needed because there is concern that the principle "allows for a fairly broad margin of judgement."[173] Within the judgement is an assessment of

---

166 *Id.* at 449-451.

167 *Id.* at 446 ("The principle of proportionality is an ex ante analysis, rendering ex post facto consequences [.]") (emphasis omitted).

168 *Id.* at 451-52.

169 *See* Michael Schmitt, *Uncertainty in the Law of Targeting: Towards a Cognitive Framework*, 10 HARV. NAT'L SEC. J. 148 (2019).

170 *Id.* at 152 ("[This] article offers a cognitive framework for thinking about the confluence of uncertainty and the [IHL] rules governing targeting.").

171 *Id.* at 167-8.

172 *Id.* at 173. The article displays this formula as: Σ [$V_{CIV} \cdot P_{CD}$] (Σ= total collateral damage concerns [V_{CIV}= value attributed to each civilian or civilian object · P_{CD}= probability of collateral damage to each civilian or civilian object].

173 *Id.*

many factors; among others, location, terrain, nature of the object, and impacts it will have once destroyed.[174] The factors eventually boil down to an assessment of foreseeable collateral damage.[175] As discussed above, this foreseeable analysis must be done in good-faith, thus the formula may provide discipline in the analysis. He notes that the impacts of data loss and inter-operability would still be difficult for value assignment, but at minimum, the formula may allow a commander to attribute value to effects such as death or injury that flow from such data loss and interoperability.[176]

Lastly, although not dealing specifically with the LOAC, Yavar Bathaee, in his article, *The Artificial Intelligence Black Box And The Failure Of Intent And Causation,* [177] provides that many legal definitions and rules that are applicable to humans may be extremely difficult to apply to AI and ML; since "[m]achines and computers have no intent."[178] This is due to legal definitions and rules' reliance on elements such as the actor's state of mind (*scienter* or *mens rea*).[179] This is applicable in terms of this article because without understanding the Black Box of AI and ML and the results that follow its employment, a commander may have an inability to reasonably make a decision regarding expected damage and its contribution to a direct and concrete military mission. As mentioned above, a commander must weigh all available information and make a good-faith decisions based upon it.[180] As Mr. Bathaee explains, intent requires scienter; the scienter of intent—here, reasonableness regarding expected damage and contribution to a direct and concrete military mission—may not be established on this premise of misunderstanding.[181] This

---

[174] *Id.* at 168-69.

[175] *Id.*

[176] *Id.* at 173.

[177] *See* Bathaee, *supra* note 104.

[178] *Id.*

[179] *Id.* at 906 ("Intent tests appear throughout the law and have developed over centuries to help courts and juries understand and regulate human conduct.").

[180] *See* Solis, *supra* note 126, at 303.

[181] *See* Bathaee, *supra* note 104, at 912.

could subject a commander to discipline if she decides to employ a weapon system without the appropriate *ex ante* analysis required.[182]

In his article, Mr. Bathaee uses the examples of an AI and ML platform used in the financial market. The platform executes a campaign to make profit from its owners.[183] The platform was programmed to devise a profitable strategy for trading equities.[184] The platform blends elements of social media, spoof-trading, and legitimate purchases to drive up the price of its shares by using those separating lines in gradients of data.[185] The value rises and crashes, however, the AI has made its move beforehand based on its aggregate actions and has made a profit. The designer who programmed the platform to devise a profitable strategy is charged with a number of financial crimes, which require proof of criminal intent.[186] Mr. Bathaee argues that intent could not be proven because the designer did not have that specific criminal intent which was involved when designing the AI and uploading data samples for the ML process.[187] The platform made these tactical decision to execute its overall strategic goal. Even if reverse engineering where to occur, the opaqueness of which separating lines within gradients of data are used is highly unlikely to be seen or understood by investigators.

Like Mr. Bathaee's example, the intent element in proportionality requires a belief that a result would follow a decision based on available data.[188] If there is no understanding as to the expected result due to a platform's technological sophistication, again, the *ex ante* analysis cannot prove that it was conducted responsibly.[189] Therefore, the good-faith intent might not be satisfied.

---

[182] *See e.g.,* DoD 2311.01E (2014) at ¶ 4.4 ("All reportable incidents [alleged violations of international or domestic law]…are to be reported promptly, investigated thoroughly, and, where appropriate, *remedied by corrective action*."); *see also* 18 U.S.C. § 2441 (a) (2006) ("Whoever, whether inside or outside the United States, commits a war crime, in any of the circumstances…shall be fined under this title or imprisoned for life or any term of years, or both, and if death results to the victim, shall also be subject to the penalty of death.").

[183] *See* Bathaee, *supra* note 104, at 911-12.

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.* at 913 ("The only intent we can examine is the designer's, and there is no intent that the designer intended that the [AI] engage in [a] particular strategy.").

[188] *See* Additional Protocol, *supra* note 7, at art. 51(5)(b).

[189] *See* Solis, *supra* note 104, at 303 (discussing the all available information test).

What can be gathered from academic discourse is that a certain level of leeway is given to commanders in their proportionality analysis. Only clear violations based upon all information available will be second-guessed. This process of evaluating all information is difficult because legal definitions and use of terms is unsettled by doctrine. The underlying functionality of a data infrastructure may be a starting point to consider in proportionality analysis's casualty and damage assessment, especially if tied to the initial impact on the infrastructure. Development of more (interdisciplinary) cognitive frameworks may be helpful. However, an appropriate assessment may not be possible given the opaqueness of the technology used. This may impact any good-faith assumption about whether a decision contributes to a concrete and direct end goal—this is a flaw in this legal system because these assumptions are based upon intent, the ultimate arbitrator of accountability for military action.[190]

C. Application

1. Past Practice

QC, AI, and ML will change proportionality analysis because it may interfere with the subjective test required by commanders, as well as result in excessive damages that appear to cross the threshold under the interpretations noted above. Indeed, those brief interruptions of network services, etc. do not violate the principle, but a *permanent* loss of an entire national-economy based upon the *uninformed* actions of one commander, and an inability of an adversary to begin recovering from the effects on civilian infrastructure, may do so. This conclusion can may be shown through past practice.

For example, in 2007, Estonia suffered an intense "distributive denial of service" (DDoS) attack, an attack designed to swarm and overrun internet traffic on servers resulting in a shut-down, in response to the county's efforts to remove a Soviet-era World War II memorial.[191] The attack resulted in massive delays and inoperability of large sectors of the economy.[192] Although widely disruptive and annoying, this was not considered a violation of international law in terms

---

[190] *Id.* at 303.

[191] Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?*, Foreign Policy, Apr. 27, 2017, https://www.foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

[192] *Id.*

of proportionality; because first, the Estonian government considered the attack an act of terrorism,[193] and second, the attacks did not amount to an "attack" because no kinetic damage resulted that would allow an analysis of the first-order or second-order effects.[194]

In 2008-2009, Georgia suffered a blend of cyber-attacks and traditional kinetic operations when "Denial of Service" (Dos) and DDoS attacks were aimed at the country's president and government websites.[195] These events were coordinated to occur at the same time Russian forces were engaged in ground combat with Georgian forces.[196] The attacks were aimed at shaping public opinion through information operations which promoted Russian narratives and vandalized government websites.[197] Notwithstanding the *jus ad bellum* issue as to the appropriateness of Russian forces invading a neighbor's country, this instance is not considered a violation of international law when analyzed with a cyber perspective of proportionality.[198] Indeed, there existed a traditional military kinetic operation, but the cyberspace actions are to be examined separately to determine their nature under the proportionality rule. The facts were too vague to conclude attribution to the Russian government and the cyber actions' impact on the country, via the first-order and second-order effects that would constitute a prerequisite "attack" for a proportionality analysis, temporary stops in services and defacing of websites, was not enough.[199]

In 2009, the country of Kyrgyzstan had two main servers come under a DoS attack that shut down websites and email within the country.[200] The DoS attacks were traced back to Russia, and coincidentally occurred during the time Russia was pressuring Kyrgyzstan to stop its support of U.S. airbases in the country for U.S. use in its Afghan campaign.[201] Attribution could

---

193 Carl Fitz, *All Is Fair In Love And CyberWar: International Law and Cyber-Attacks*, HOUS. J. INT'L L. SIDEBAR (2017), http://www.hjil.org/wp-content/uploads/Fitz-FINAL-1.pdf.

194 *Id.* at 8-10.

195 William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, SCHOOL OF ADVANCED OF ADVANCED MILITARY STUDIES, UNITED STATES ARMY COMMAND AND GENERAL STAFF COLLEGE 11 (2008-09), https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-027.pdf.

196 *Id.*

197 *Id.*

198 Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 18-19 (Nov. 2008), http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf.

199 *Id.*

200 *See* Ashmore, *supra* note 195, at 13.

201 *Id.*

not be proven, and again, the impacts amounted to mere annoyances and temporary shutdowns—far below the first-order and second-order effects needed to analyze proportionality.

In 2010, there was the discovery of a malicious code dubbed *Stuxnet.*[202] This presented the one of the first instances of physical damage related to a cyber campaign.[203] The attack, which targeted Iranian nuclear facilities through its Supervisory Control and Data Acquisition (SCADA) system, resulted in physical infrastructure loss of functionality—again, with physical damage—and a spread of the code to other parts of the country and around the globe.[204] Although the loss of functionality may have been the intent and goal of whomever used the code to attack Iran, it was most-likely not intended for the code to spread to other areas around the globe and damage others' data infrastructure. This highlights the deleterious results from a lack of technological understanding as to how and why a platform or tool will execute a strategy in a particular way. In other words, the expected infections to others outside of the intended target cannot be valued against the mission because they are unknown considerations. This may have violated proportionality because the "knock-on" effects where not fully understood, as well as the later "knock-off" effects, in effect rendering proportionality analysis incomplete.[205]

Lastly, from 2014 to the present, we have seen a string of cyber-related attacks and uses of advanced technologies as a means of operations for nation-states. The Ukrainian war on its eastern border displays forms of Russian state military doctrine of "hybrid warfare"—the use of information operations on the general public, electronic warfare, cyberwar, and other forms that impacts all layers of the cyber domain, as well as traditional kinetic operations.[206] The civilian population not only suffers routine physical damage from the kinetic operations, but suffers the same fate as those in the Georgian, Estonia, and Kyrgyzstan.[207] So far, international law discourse has considered these actions within the "grey zone" in terms of *jus ad bellum* and *jus in*

---

[202] *See* John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. MARSHALL J. COMPUTER & INFO. L. 1, 5 (2001).

[203] *Id.* at 5-7.

[204] *Id.; see also* P.W. Singer, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, 47 CASE W. RES. J. INT'L. 79 (2015), 81-82.

[205] *See* Richardson, *supra* note 202, at 24-26.

[206] *See* George Perkovich & Ariel E. Levitte, *Understanding Cyber Conflict: 14 Analogies*, Georgetown Univ. Press, 85-93 (2017), https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch5.pdf.

[207] *Id.*

bello because their relation to the legal margins of what constitutes a real hostility.[208] In isolation, these attacks present the same form of annoyance, but prolonged loss of functionality and "knock-off" kinetic effects (including proximate cause civilian casualties that flow from this loss of functionality) may violate proportionality's "excessiveness" and "expected damage" rule.[209]

From these examples, it seems that physical damage fits into the classical proportionality test. New considerations may be needed within this grey-zone of legal interpretations to cope with extended or permanent loss of data and interoperability of systems, as well as harms to civilians and their property as a result. Moreover, whether such permanent loss of data and interoperability of systems can be accurately assessed from available battlefield information and understanding of weapon system employment.

2. Hypothetical Revisited

In any of these situations, the introduction of QC would make it highly unlikely these victim-States would have suffered brief, non-permanent damage. The damage may not fully be capable of responsible prediction, leading to the expected damage outweighing the mission goal. If Estonia had continued to suffer the deprivation of its national economy for a prolonged period of time rather than minor annoyances; if Georgian citizens were unable to rely on government services that provided health, safety, and utility services for months as a result to damaged government websites; or if Kyrgyzstan government would have been unable to perform basic works on behalf of its citizens as an impact from server shutdowns, the analysis may yield a result different than the above real-world conclusions, which may violate the principle of proportionality.[210]

The implementation of the weapon system mentioned in the introductory hypothetical would cause these annoyances to become real second-order effects in the face of a weapon system that continually thinks and predicts adversary movements faster and in a more capable manner that is required to recover. The AI, ML, and QC tool would have trained on sets of data analyzing enemy behaviors and predicted their troubleshooting methodologies and identified unknown vulnerabilities of the adversary system for purposes of meeting military strategic goals of

---

208 *See, e.g.*, Michael Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1 (2017).

209 *See* Additional Protocol, *supra* note 7*,* at art. 51(5)(b).

210 *Id.*

the attack. This included the entire civilian communication infrastructure. The tool pulls from those gradients in data, analyzes the data through the many neurons and layers within its system, finds hidden patterns within the data, produces algorithms to accomplish its goal, and executes with a speed and tempo faster than modern computing methods can cope. Current encryption schemes and troubleshooting methods to break QC's post-quantum encryption regimes will be of no use. Impacts and effects would potentially result in real civilian casualties and damage to infrastructure.

Recall that proportionality contains four elements: 1. there must be an attack; 2. an expected civilian loss of life, injury, or damage or a combination thereof; 3. a concrete and direct military advantage is anticipated for the action (attack); 4. the expected civilian loss of life, injury, damage to civilian objects, or a combination thereof, is excessive compared to such concrete and direct military advantage.[211] If a decision to conduct an operation fails to satisfy these proportionality elements, the attack must be cancelled or postponed.[212] Pulling from the proportionality analysis requirements, an attack must be present because the physical degrading of the communications system's infrastructure occurs as a "knock-off" effect of the operation.[213] Moreover, there is an expectation that there would be at-least some form of damage to civilian objects, the damage is in the form of loss of functionality and physical degradation of the system. This loss of functionality would not initially be excessive because annoyances and short periods of disruptions, as well as losses to data are not considered excessive under current doctrine and understanding of the principle of proportionality. Lastly, a concrete and direct military advantage of stopping adversary command and control is present. This military advantage serves the purpose of striking the adversary's critical vulnerability of efficient coordination between its forces.

One issue with the hypothetical lays within the fourth element, whether there is an *expectation* of excessiveness compared to the military advantage. In order to conclude that there wasn't, the commander would have to make a reasonable and good-faith judgement as to its at-

---

211 *Id.*.

212 *Id.*

213 *See supra* Section I. B.

tack's potential effects.[214] This is based on all available information at the time.[215] She may have initially concluded there would only be minor annoyance of loss of functionality for purposes of disrupting enemy command and control movement, making this attack compliant with international law.[216] The attack would stop where she wanted it to. She most likely did not expect to capture a national economy, a result flowing from a misunderstanding of the weapon system's inner AI, ML, and QC workings.

Although an argument exists that the result cannot be imparted on the commander because the weapon system's AI made this strategic choice outside of the commander's true intent, it may not work in terms of the proportionality rule. The responsibility of accurately assessing *all* data available would include the weapon system's inner workings. If the commander did not understand the inner workings of the system, she could not truly make a reasonable decision based on *all* available data—those algorithms, separations in data, and gradients used for the system's decision-making process. This would also raise questions as to whether a good-faith decision was made, given the reality that expected results are uncertain, or whether a decision was mere guesswork.

Another issue is present in the level of excessiveness compared to the concrete and direct military advantage. If the civilian systems merely suffers loss of functionality for a short duration, the commander may still be in the clear given precedent found in this article's examples and academic interpretations. However, if new computing methods such as QC extend this loss of functionality into perpetuity or a crumbling of the national economy and services, there may be an immediate paradigm shift as to the damage compared to the goal of stopping adversary coordination. Without the inability to recover in the face of the computing (quantum) supremacy and battlefield singularity maintained by the commander and her weapon system, the damage could slowly creep into the realm of "clear" excessiveness.

On that note, the commander may have subjected herself to disciplinary liability by making an uninformed decision as to the reasonableness and good-faith of her decision.[217] Ac-

---

[214] DOD LAW OF WAR MAN., *supra* note 8, at § 5.3.

[215] *See* Solis, *supra* note 126, at 303.

[216] DOD LAW OF WAR MAN., *supra* note 8, at 1022.

[217] See DoD 2311.01E, *supra* note 182; *see also* 18 U.S.C § 2241, *supra* note 182.

cording to international law, the attack should have been cancelled or suspended, *ex ante*.[218] The other result could be that this hypothetical is merely extensive in damage and that the commander did all that she could; essentially, Black Box AI, QC, and ML execution is understood by none. This would shift the paradigm back to the discourse of uncertain responsibility, which that may be of no help to anyone.

V. Normative Solutions

New impacts on proportionality may be managed through responsible organizational control of the decision-making process and criteria, based on available information. The above hypothetical and its results can be mitigated with a group of general normative principles. There are potentially many solutions available, for sake of brevity, this article provides the below.

A. Understand the Technology, How it Works, and Why it Chooses Certain Actions to Accomplish Goals: "If you know, you know"

The information assessment standards of proportionality requires the party executing an attack to understand the inner workings of QC, AI, and ML.[219] They must understand what the data sets consist of, understand the gradients and how they are used, how weight is assigned, and how they are measured within those layers' neural networks.[220] Lastly, they must test the weapon system to understand how the data is being used and where those opaque separation lines are being drawn to produce variables for execution.[221]

---

[218] *See* Additional Protocol, *supra* note 7, at art. 57(a)(iii).

[219] *See supra* Section IV.

[220] *Id.*

[221] *See* Bathaee, *supra* note 104, at 928-9.

B. Retain Effective Control of the Technology and its Ability to Choose Pathways of Action to Accomplish Goals

Observe, orient, *decide*, *act,* and repeat.[222] This may be a rehashing of the "humans in-the-loop"[223] argument, but end-state decision making should never be delegated to a weapon system by algorithm or any other method.[224] The potency of battlefield singularity that AI and ML bring to a fight, as well as the computing (quantum) supremacy of QC, can produce deleterious results which are outside the control of human actors.[225] Attempts should be made to build within algorithms specific goals to be accomplished, contain markers that signal when an attack should stop, and when a human's intent has been accomplished.

C. Ensure the Platform Uses Correct Data Sets for Training Before it is Employed and Deployed: "Appreciate, but don't discriminate"

The weapon system will only execute on data-sets it has trained on.[226] It will make tactical and strategic decisions based on pattern recognition and past practice.[227] Close attention should be paid to military precedents, race, gender, types of infrastructure, and other sensitive data. This could prevent a system from making unintended decisions based on patterns derived from questionable training data sets.[228]

---

[222] Referred to as the "OODA-Loop", it is a decision matrix originally used and developed by Air Force Colonel John Boyd for military professionals. It is now used by a variety of professional communities. *See, e.g.*, Berndt Brehmer, *The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control*: *Assessments, Tools and Matrics,* 10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM THE FUTURE OF C2, DEPARTMENT OF WAR STUDIES, SWEDISH NATIONAL DEFENCE COLLEGE (2005), HTTP://WWW.DODCCRP.ORG/EVENTS/10TH_ICCRTS/CD/PAPERS/365.PDF (last visited April 11, 2019).

[223] *See* Alan L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARVARD NAT'L SEC. L.J. 379 (2017).

[224] *Id.*

[225] *See* Ashley Deeks, Noam Lubell & Daragh Murray, *Machine Learning, Artificial Intelligence, and the Use of Force By States*, 10 J. NAT'L SECURITY L. & POL'Y 1 (2019) (Discussing legal implications of badly produced algorithms leading which may lead to an armed conflict due to such algorithms inability to contemplate legal implications of its actions).

[226] *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City,* 20 YALE J. L. & TECH 103, 113-14 (2018) (The use and creation of predictive algorithms constructed through analysis of large datasets that may reveal correlations between various features and desired or objectionable outcomes).

[227] *Id.*; *see also* Ali, *Cybersecurity Support of Insider Threat Operations*, *supra* note 72.

[228] *Id.; see also* Ali, *Cybersecurity Support of Insider Threat Operations*, *supra* note 72, at n. 373 (citing State v. Loomis, 881 N.W. 2d 749 (Wis. 2016); *see also* Brief for the United States as Amicus Curiae, Loomis v. Wisconsin, 137 S. Ct. 1240 (2017) (No. 16-6387) (Challenge to use and access to discriminatory data used in recidivism analysis of sentencing hearing).

D. Create End-Goals that Promote Expected Results: "Inspect what you expect"

Goals for a weapon system should not be vague or open-ended.[229] They should be real, achievable, and narrowly-tailored to meet the charged human's intent. In fact, AI and the process of ML are generally considered at their best performance when goals and missions are narrowly tailored.[230] The process usually involves taking "*x* and [adding] AI."[231] For example IBM's *Deep Blue* chess machine in chess or its *Watson's* performance on the television show Jeopardy.[232] AI and ML capabilities aren't yet scalable to take on general intelligence problem sets—such as that of interpreting end goals.[233] This won't be the case forever, especially considering the concept of an AI superintelligence explosion, defined as the point in which AI surpasses humans in general intelligence.[234] For now, limited and narrowly-tailored goals should be the same behavior for military strategy. Planned success at one level of warfare eventually influences success at all levels of warfare.[235]

E. Develop International Standards for Post-Quantum Encryption: "Defense wins championships"

" With that said, the inevitable arrival of QC and its uses in military operations should promote the development by military and civilian communities of post-quantum cryptology in the form of quantum resistant algorithms (QRAs) and quantum random-number generators (QRNGs).[236] QRAs are expressed in the form of quantum resistant algorithms that use difficult math equations, and QRNGs are expressed in the form of truly random numbers generated by naturally occurring randomness (think measurements of solar flares), that are useful enough to stall or prevent QC from disrupting whole infrastructures for tactical gains.[237] The National Insti-

---

229 *See* Hague Convention (IV), *supra* note 106, at art. 23(e).

230 *See also* Ali, *Cybersecurity Support of Insider Threat Operations*, *supra* note 72, at n. 229.

231 Kevin Kelly, *The Three Breakthroughs That Have Finally Unleashed AI on The World*, WIRED BUSINESS, (Oct. 27, 2014), https://www.wired.com/2014/10/future-of-artificial-intelligence/.

232 *See* KASPAROV, *supra* note 5; MAX TEGMARK, LIFE 3.0: BEING HUMAN IN THE AGE OF ARTIFICIAL INTELLIGENCE 78, 161, 259 (Penguin 2017).

233 *See, e.g.*, NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGER, STRATEGIES (Oxford Univ. Press 2014).

234 *Id.*

235 *See, e.g.*, U.S. MARINE CORPS, *supra* note 1, at 28-31.

236 *See* Herman & Friedson, *supra* note 21, at 12.

237 *Id.*

tute of Standards and Technology (NIST) has begun this process, but projected timelines for market and capability confidence has the potential to be surpassed by the development of an operational quantum computer.[238] More serious attention and effort must be given to this matter for public, commercial, and government access.[239]

Another possible solution is the implementation of Lattice based cryptography.[240] Lattice based cryptography uses constructions of algorithmic protocols used to build cryptology—the backbone of computer security systems—by relating their construction to proofs of *very hard* math problems.[241] This is sometimes referred to as "worst-case hardness."[242] Lattices are spaced grids of an evenly distributed, but infinite number of vectors.[243] Connecting these vectors results in coordinates.[244] These coordinates can have multiple beginnings, interconnecting in an infinite number of ways.[245] As related to QC and its ability to efficiently factor large integers, Lattice present an infinite number of problems sets (coordinates) for a computing methodology (QC) which is at-least theoretically, finite.[246]

Essentially, these Lattice schemes are built with security resiliency in-mind. If Lattice cryptology is used, it could present QC, even if using ML methodologies, with an efficiency factoring problem it cannot accomplish its computing goals in time for whatever goal its designer had at the time.

F. Develop Consistent Legal Terminology and Framework: Clarity breeds confidence

The development of agreed upon legal terminology, even in the form of an "Additional Protocol IV"—as Commander Pascucci notes in his aforementioned article—could establish thresh-

---

238 *See* LILY CHEN, ET AL., NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COM. REPORT ON POST-QUANTUM CRYPTOGRAPHY 6 (2016), https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (last visited April 20, 2019).

239 *See* Herman & Friedson, *supra* note 21, at 12.

240 See DANIELE MICCIANCIO & ODED REGEV, LATTICE-BASED CRYPTOGRAPHY, New York University (2009).

241 *Id.* at 2.

242 *Id.* at 3.

243 Joël Alwen, *What is Lattice-Based Cryptography & Why Should You Care*, MEDIUM (June 15, 2018), https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717.

244 *Id.*

245 *Id.*

246 *Id.*

olds for collateral damage and certainty of effects in the cyber domain.[247] This could also be applied to terminology that describes when a system is devoid of operability or when data erasure constitutes excessive damage. This could possibly be added to Professor Schmitt's mathematical formula for proportionality.[248] This could also face resistance, as the elastic concept may be more adept at addressing operational goals in a conflict—winning—but a more disciplined approach in providing clarity of terms may assist in accomplishing operational goals in a legally sufficient manner.

VI. Conclusion

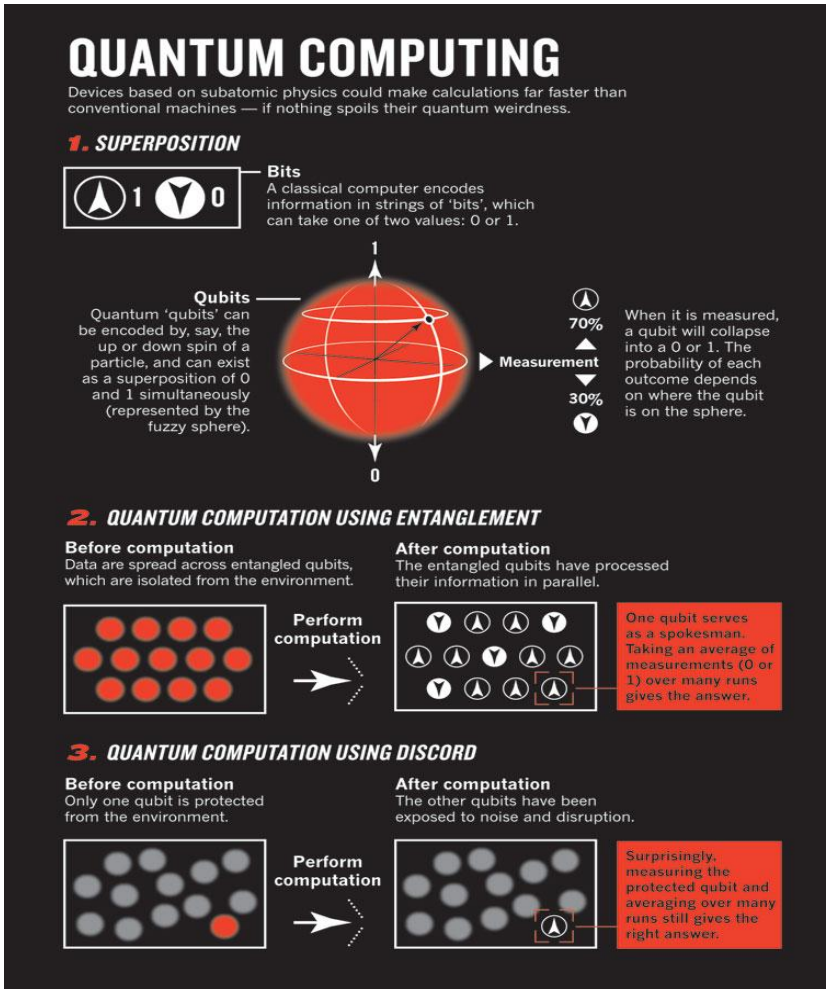
The proportionality principle is elastic and flexible. This elasticity and flexibility may not be adept at providing responsible and legal decision-making in the face of advanced technologies. These decisions demand reasonable and good-faith conclusions to be made based upon data. The use of AI, ML, and QC may not allow for this if there is no effective control or understanding as to why weapon-systems choose courses-of-action outside what is needed for a military mission. Nor is the standard met with mere guesswork as to the unpredictable and potentially excessive impacts to civilians and property. This can be remedied with appropriate levels of legal integrity and frameworks in the employment of this technology by looking to, and learning from, doctrine, past practice, academia, and current practice.

---

[247] *See* Pascucci, *supra* note 120, at 456-7.

[248] *See* Schmitt, *Law of Cyber Warfare, supra* note 145, at 297-99.

APPENDIX I: Qubits



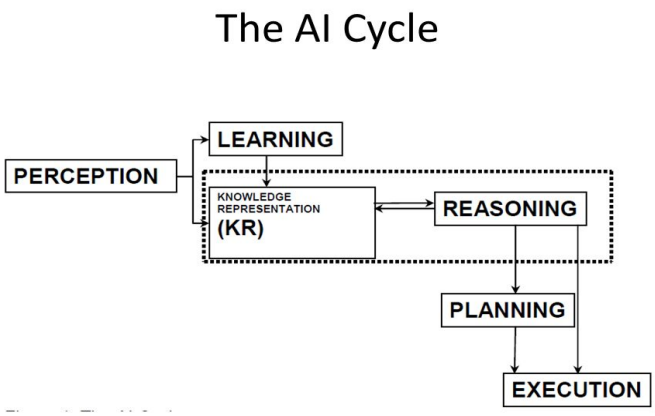
This figure adopted from an online article by Abhishek Ghosh, *IBM Brings Quantum Computing in the Cloud*,[249] shows that *quibits* bring a different dimension to computing. The figure shows how a *qubit* can exist in each state (1 and 0) at the same time due to its encoding within a physical property. The physical property is measured and gives a variable as a one or zero. The probability that it is a one or zero depends on where the data resides within the physical property at the time of measurement. For national security purposes, once measured, the *qubit* collapses as either a one or a zero; this would indicate someone or something is attempting to figure out what is within the *qubit*. The collapsing state is an indication of possible infiltration attempts by an adversary.

Entanglement and Discord offer their own protections such as processing information in parallel and protecting information from exposed noise and disruption. Just like that of superposition, the national security implications are evident.

---

[249] Abhishek Ghosh, *IBM Brings Quantum Computing in the Cloud*, THE CUSTOMIZE WINDOWS (May 5, 2016), https://thecustomizewindows.com/2016/05/ibm-brings-quantum-computing-cloud/.

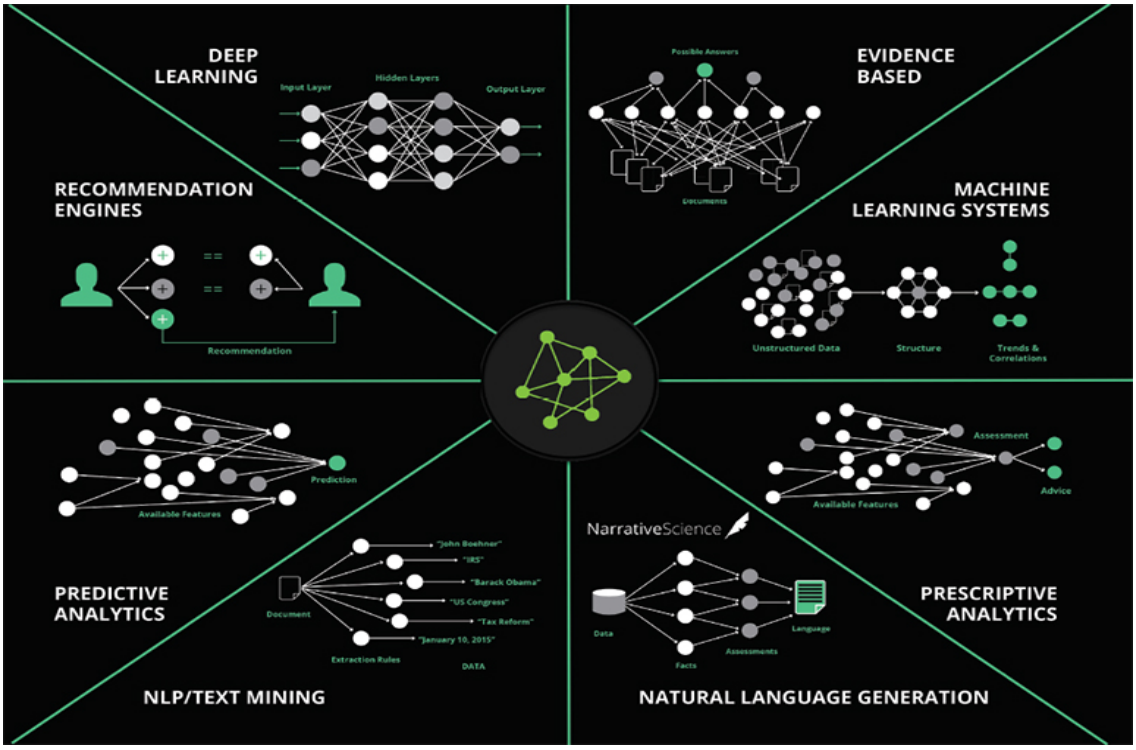
APPENDIX II: Artificial Intelligence Cycle



The above figure adopted from an online presentation, *Artificial Intelligence Knowledge Representation*,[250] by Hillary Ross, demonstrates a basic framework for AI decision-making. An AI platform perceives its environment, processes its perceptions of the environment, stores it as data, analyzes the data and plans the best course-of-action via programmed algorithms, and decides on a method or tactic to accomplish the assigned goals. For purposes of this article's discussion, an AI platform would have been the recipient of pre-programmed data sets and examples to assist it in this decision-making process of attacking enemy communication infrastructure. For instance, it may have been programmed with infrastructure penetration tactics and malicious codes to best exploit enemy system vulnerabilities. This process serves as a framework for executing QC.

[250] Hillary Ross, *Artificial Intelligence Knowledge Representation*, Slide 6/18, SLIDEPLAYER (last modified 2016), *https://slideplayer.com/slide/8088670/*.

APPENDIX III: Machine Learning



The above figure adopted from the online article, *Inside the Black Box: Understanding AI Decision-Making*,[251] by Charles McLellan, demonstrates the myriad approaches to machine learning. It is best understood that this process mimics the human brain by passing data through multiple interconnected neurons that process and weigh data for consideration. Each neuron may carry simple mathematical operations, but together, they can potentially generate algorithms based on patterns that are too opaque for humans to see. For example, the tool used in this article's example may have caught gaps and exploits unnoticed by the adversary's infrastructure managers. It has also decided, based on these gaps and patterns, to keep exploiting the entire system to prevent any troubleshooting. This process facilities and supports QC and, even if the adversary had its own AI/ML defense systems, the ability to compute at a more powerful rate would render such defense system moot.

---

[251] Charles McLellan, *Inside the Black Box: Understanding AI Decision-Making*, HOW TO IMPLEMENT AI AND MACHINE LEARNING, ZDNET, Special Feature (December 1, 2016), *https://www.zdnet.com/article/inside-the-black-box-understanding-ai-decision-making/*.