Phalanx close-in weapons system aboard *Ticonderoga*-class guided-missile cruiser USS *Cowpens* fires at missile decoy, September 10, 2012 (U.S. Navy/Paul Kelly)

Autonomous Weapons Systems Safety

By Brian K. Hall

If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner.

—General Omar Bradley

Looking to the future to identify strategic trends, continuities, and projected policy, as well as planning and force development strengths and deficiencies, the joint force must contend with the rapid diffusion of advanced technology economically and commercially available to non-superpower militaries and the profusion of nonstate actors. To contend with this problem set, we must reassert our national lead in safely developing military capabilities to withstand a future security environment that is likely to be more unpredictable, complex, and potentially dangerous than today.

One way to deal with such an operational challenge is to design and field force options comprising a mix of capabilities that proportionately includes greater integration of autonomous systems. What will influence our ability to direct such a strategic shift is policy

Colonel Brian K. Hall, USAF (Ret.), is the Autonomy Program Analyst for the Force Application Division, Joint Staff J8 (Force Structure, Resources, and Assessment).

guidance and oversight for the development and employment of autonomous systems—particularly weapons systems—with lethal capability.

Available technology and unforeseen world events will make it increasingly difficult to apply the law of armed conflict and international law relating to the use of force via autonomous weapons systems in a consistent manner that adheres to U.S. policy.

Many nations, including the United States, will place limits on the use of lethal autonomous weapons systems (LAWS) to avoid the risk of collateral damage and to comply with international humanitarian law. However, potential adversaries might not be bound by these constraints. The joint force may confront adversaries who are willing to deploy fully autonomous weapons systems to deliver lethal force and more completely automate their kill chains to achieve an advantage. The potential exists that in such a situation the United States and like-minded nations will be more willing to enter conflict or use lethal force given the lower potential of loss of their own combatants through the use of either autonomous or semi-autonomous weapons systems.

Ultimately, commanders and operators will exercise appropriate human judgment over the suitable use of this force.

This article furthers the technical issue discussions supporting the emerging U.S. position to the United Nations Convention on Certain Conventional Weapons on LAWS. It also addresses the current U.S. military joint weapons review practices that lead to weapons safety assurance and endorsement for any weapons system—manned, autonomous, or semi-autonomous. The article emphasizes safety and trust by determining operational necessity, averting risk, and applying engineering design reliability. This practice is consistent with current U.S. defense policy cited in Department of Defense (DOD) Directive 3000.09, "Autonomy in Weapons Systems." Readers should better understand the precautions taken to prevent unintended machine action and function of a lethal nature.

State of Autonomy

Autonomy is often misunderstood as providing independent thought and action. For weapons systems, it most often suggests self-awareness and self-governance.

Autonomy is better understood as a technologically advanced capability or capabilities that enables the larger human-machine system to accomplish a given mission by the performance of key actions—with or without human intervention.

In this instance, autonomy is not exclusively about the intelligence of the machine but rather its human interface.

The degree of autonomy in a single human-machine or machine-machine system may vary over time as it goes in and out of contact with operators. The dynamic relationship between technical needs and capability benefits demonstrates that the level of autonomy of a system is not a goal in and of itself. Rather, autonomy is a capability driver that DOD can design into military systems in conjunction with human roles to produce a more effective and affordable force. Autonomous systems will reliably perform highly survivable, self-organizing, adaptive mission capabilities that cannot be easily defeated either by killing individual platforms and sensors or providing capabilities to do things that would be otherwise unaffordable or result in impractical manning.

The 2015 Office of Technical Intelligence report, *Technical Assessment: Autonomy*, illustrates control diversification between man and machine from an engineering *coupling* approach:

Viewing the capabilities of autonomous systems within the context of human-machine systems recognizes a critical role for humans coupling the advantages of both allowing for operational application previously non-existent. In order to better capitalize upon the relative strengths of humans and machines, autonomous systems will operate on a spectrum from tightly coupled to loosely coupled. Where human performance provides benefits relative to machine perception, cognition, or action and where safety and risk to warfighters is acceptable, autonomous systems will benefit from being more tightly coupled with humans. Often, tightly coupled systems will feed information directly to humans, such as automatically cueing a warfighter to a threat or analyzing large amounts of electronic emissions and presenting exploitation options to human analysts and planners. For missions where humans are less effective or which are too dangerous and remote control is not feasible, more loosely coupled systems will operate with less input from human operators. These more closely fit the traditional conception of autonomous systems—those that operate while out of touch with humans, such as a strike platform in a communications-degraded or denied environment.

Some of the greatest advantages of autonomy will come from augmenting human decisionmaking, not replacing it. In this way, the role of humans will aggregate at the higher cognitive processes such as operational planning and analysis. As such, human-machine interaction is a key technology area supporting autonomy.

Increased automation or autonomy can have many advantages, including increased safety and reliability, improved reaction time and performance, reduced personnel burden with associated cost savings, and the ability to continue operations in communications-degraded or -denied environments.

This article recommends a sound U.S. weapons review practice that will, with minor modification following autonomous technology sector growth, enable balanced autonomous system capabilities to be advantageously included in future operations. This discussion does not attempt to directly address future policy or legal changes that may be required to ensure inclusion of an advanced unmanned capability into force development, posture, and employment. Doing so would be premature; how the confluence of autonomous weapons system policy with legal and technical factors will impact the conduct of future warfare is not yet known. What could be done is help shape what it could be. The international community is watching how the United

Researchers with U.S. Army Natick Soldier Research, Development, and Engineering Center are testing Prox Dynamics PD-100 Black Hornet Personal Reconnaissance System to provide squad-size units with organic aerial ISR capability in challenging ground environments (Courtesy UK Ministry of Defence)

States contends with these emergent technologies and integrates them into force design, development, and employment. Doing so has far-reaching global strategic security implications.

Advances in science and technology—such as artificial and collective intelligence, miniaturized sensors, multivehicle control systems, and particularly human-machine interaction—are laying the foundation for giving autonomous weapons the ability to perform at levels currently difficult to predict. Weapons review, appropriately applied, ensures safety of such capability across the range of operations, both civil and military. Autonomous systems will become part of the social landscape, and as autonomy and computational intelligence grow, these systems will continually raise difficult questions about the role of safety and effective integration with humans. As weapons systems, particularly those with greater autonomous capability, are studied and understood, society will face challenging policy and regulatory issues surrounding how much autonomy these systems should be granted based upon acceptable levels of risk. Ultimately, the path of these technologies is dependent upon rational human judgment when delegating mission capability to autonomous systems.

Diversification and Operational Risk

DOD has diversified and invested in considerable numbers of unmanned vehicles over the last several decades. Today, the inventory stands at well over 20,000 unmanned vehicles spanning all domains, at a fiscal year 2017 budgeted funding level of $4.5 billion.[1] Projections estimate that by 2018, annual global spending on military robotics will exceed $7.5 billion.[2] These vehicles are integrated elements of varying degree of larger robotic and autonomous systems used for a variety of missions, including persistent surveillance, firefighting, time-critical strike, force protection, counter–improvised explosive devices, route clearance, and close air support. Conceivable tasks for future autonomous systems of all domains span the full range of military operations.

The diversification is not unprecedented, and such endeavors should be undertaken with cautious optimism. The United States explored various technologies during the Cold War–era to define the emerging nuclear-space age. For example, in a determined move to diversify its defense business base in the 1950s, General Motors scaled tank and gun production favoring new markets in military electronics.[3] Others followed a similar strategy to include Lockheed, Northrop, Martin, and Douglas Aviation. This diversification spread through the defense sector, spawning advances in the missile and electronics fields that became the technological keystone of the DOD First Offset Strategy. The United States and its mission partners find themselves in a similar revolution in military technology brought on by innumerable robotic and autonomous technologies that are shaping the character of future warfare. Innovative concepts of operations and wargaming are just now revealing the previously unrealized human-machine teaming potential of these robotic and autonomous systems.

The technologies that enable autonomous systems are evolving rapidly. As computer processing power and sensors improve, autonomous systems will be capable of increasingly complex decisions and actions. The ability to operate

in fast-paced, contested, nonpermissive, force-on-force engagements, particularly under conditions of degraded communications, will drive the need for increased autonomy. The United States already has autonomous force protection systems that defend bases and ships against air and missile attack (for example, Counter Rocket, Artillery, and Mortar; and Phalanx). Which decisions are appropriate for delegation to autonomous systems and which must be retained under human control will be important considerations for defense policymakers. The fact that the U.S. military has had defensive systems that autonomously use lethal force for decades complicates the issue on the use of force. The track record of these systems suggests that safeguards are required in order to minimize the probability of civilian casualties, premature application of force, fratricide, or unintentional escalation.

Autonomous systems are vulnerable to an array of potential failures, including situations common to any software-dependent system, as well as additional failures due to their scalable complexity. As the complexity of a system increases, so does inherent operational risk. Verification (the ability to meet system requirements) and validation (the ability to operate as intended) of software to ensure trustworthy, reliable operation become imperative. Currently, it is increasingly difficult for operators to predict with a high degree of probability how a system might actually perform against an adaptive adversary, potentially eroding trust in the system while asserting operational risk. To avert risk and instill trust, it becomes increasingly important to invest in autonomous weapons system modeling, simulation, and experimentation to explore the fast-paced, complex, unstructured environments that autonomous systems may face in future scenarios. Also requisite to achieving assured autonomy are rigorous test and evaluation to develop a deep learning database of successful actions and problem-solving computation and recall.

It is widely recognized that systems relying on software are vulnerable to cyber attack from many vectors. A successful cyber attack could conceivably allow an enemy to disable mission-critical operation or, in a worst-case scenario, usurp control of an autonomous weapon. Today, autonomous systems, to varying degree, are vulnerable to spoofing, hacking, and intrusive deception measures in ways that humans are not because artificial mechanical systems lack self-awareness, common sense, and a general frame of reference against which to measure faulty data. Safeguards and fail-safes are needed to minimize the probability and impact of compromise or failures that could lead to unintended consequences resulting in damage to persons or things that were not deliberately targeted.

DOD currently depends on policy guidance in autonomy, human control, and the use of force that informs military tactics, techniques, and procedures; doctrine; minimizing collateral damage; rules of engagement; or future system design to ensure that adequate safeguards are in place. Next-generation unmanned vehicles (for example, carrier-based aerial refueling systems) and autonomous munitions (such as long-range antiship missiles) currently in development have the potential for autonomous characteristics, function, and even behavior. Current guidance is derived from many sources, as autonomy has both national defense and civil implications. Direction comes predominantly from DOD Directive 3000.09 and the department's unmanned system roadmaps and strategic plans. Other organizations within DOD and across mission partners are addressing challenges with respect to autonomous sense and avoid technologies, loss of communications procedures, static and onboard defense of manned installations and platforms, and other issues. DOD and the Department of State have a unified effort to assess current policy guidance on autonomous force application—current policy remains relevant and authoritative. But without determined guidance review to accommodate game-changing technologies forecast to reach advanced readiness levels over the next 5 years, the Nation risks obsolescence that could cede advantage to potential adversaries, permit inadequate safeguards leading to systems with the potential for unintended engagements, or both.

Operational Trust

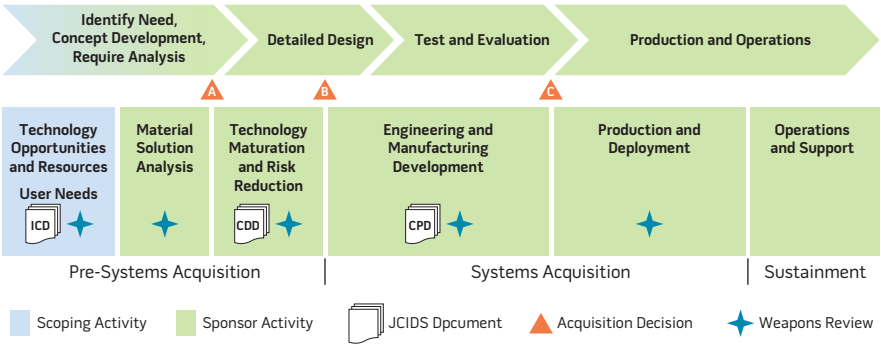
A prominent issue—potentially the greatest at home and abroad—with military employment of fully autonomous capabilities is one of trust that an autonomous weapons system will do what it is supposed to do when it is supposed to do it. If it does not, then forces in the field relying on shared task performance to assure mission success will not use the system due to lack of trust, with safety compromised. There is more likely to be trust in robotic and autonomous systems supporting these sorts of missions if they are most of the time at least partially controlled by a human or have demonstrated assured, fully autonomous mission capability during force development and training.

Part of the trust issue is that autonomous weapons systems may suffer from cyber vulnerabilities where information systems, system security procedures, or internal controls are exploited. At issue is whether an autonomous weapons system is either not functioning as it is supposed to because its algorithms have been compromised by cyber attack or system programming has been taken over to the point where it is acting against its own forces.

A related and far-reaching issue is the concern of autonomous systems properly following the orders of manned systems. There are multiple ways for issues to arise, including preplanned program malfunction and adversary jamming of sub-system intelligence, surveillance, and reconnaissance sensors and associated command, control, and communications links. The issue becomes whether there will be enough sensor precision and assured data exchange in contested and unstructured environments to allow autonomous systems to sense what they need to either take action on their own or report the information to their human operators. These are important points to consider now as we shape strategy, force design, and operational planning for the future.

Autonomy is not the sole solution to any requirement. The utility of any

Figure. Capability Requirement and Acquisition Integrated Periodic Weapon System Safety Review



autonomous capability is a function of the mission design requirements, operational environment of employment, and operational context describing how the capability will be used.[4] The prevalence of autonomy in game-changing technologies presents opportunities to expand mission capability. The emergence of these technologies challenges both capability and material developers and users by introducing distinct differences in action and function between automated (robot-like) and autonomous (cognitive-capable) systems.[5] More than likely, development of new autonomous systems will be deliberate and incremental; so too will be development of norms about acceptable system design, acquisition, and use.

Current Practice—Safety Assurance

The approach and procedures effectively institutionalized in the DOD Joint Capabilities Integration and Development System (JCIDS) provide initial system safety oversight and guidance to minimize the probability and consequences of catastrophic failure or critical mishap that could lead to unintended autonomous weapons system engagement.[6] Before any new capability can enter the development process related to reviewing and validating its requirement, the originating sponsor organization must first identify autonomous or semi-autonomous weapons system capability requirements related to its functions, roles, mission integration, and operations. Then, it must determine if pursuit of such capability presents an unacceptable level of risk and hazard as compared to qualified benefit. At this point, the weapons system concept of employment is assessed against policy and both national and international law.

Initial weapons systems safety assurance should be complete before the acquisition, engineering, and manufacturing development (EMD) phase. But it begins as early as entry-level material solution analysis (see figure) of the acquisition process—the nexus of JCIDS and the Defense Acquisition System.

In compliance with Joint Requirements Oversight Council Memorandum 102-05, "Safe Weapons in Joint Warfighting Environments," all munitions or associated systems capable of being used by any U.S. military Service in joint operations are considered joint weapons and require a joint weapons safety review in accordance with JCIDS and under Joint Service Weapon and Laser System Safety Review processes.[7] Mission capability system attributes and performance parameters must be addressed as the basis for the Weapon Safety Endorsement.[8] This includes identification of everything necessary to provide for safe weapon storage, handling, transportation, or use by joint forces throughout the weapon life cycle, to include performance and descriptive qualitative and quantitative attributes. This is important, as baseline performance measurement and system safety attributes will be integral to systems engineering—particularly test and evaluation.

In particular, compulsory assessments and reviews are captured in Capability Development Document (CDD) as part of overall weapons safety assurance required for continued acquisition decision and entry into EMD phase.[9] For example, the CDD addresses system safety in accordance with current DOD guidance,[10] confirming the establishment of a system safety program for the life cycle of the weapons system in accordance with the Defense Acquisition System.[11] This program conforms and complies with treaties, international agreements, Federal regulations, and laws. Additionally, DOD instruction provides further risk acceptance criteria.[12] This cascades into operational planning and employment decisions to include autonomous weapons system aspects in rules of engagement development and ultimately the commander's assignment of tactical mission tasks.

Furthermore, acquisition and procurement of DOD weapons systems shall be consistent and compliant with all applicable arms control agreements, customary domestic and international law, and the law of armed conflict.[13] DOD-authorized counsel shall conduct the legal review of the intended acquisition of weapons or weapons systems.[14]

Autonomous weapons system reviews, particularly of a lethal nature, are consistent with established United Nations Convention on Certain Conventional Weapons associated arms control protocols. It is premature to classify LAWS as inhuman or otherwise as the large-scale operational implications of employing such technology are just now being studied and analyzed across many defense sectors.

Rethinking Joint Function and Performance

Conventional ways to classify capabilities and their associated characteristics to accommodate the unique key system attributes of autonomy may be inadequate and require adjustment. The purpose and method behind doing so come from the realization that traditional means of command as a solely human endeavor, mechanisms for control, communications in denied

MQ-8B Fire Scout unmanned aircraft system from "Magicians" of Helicopter Maritime Strike Squadron 35 prepares for flight operations aboard littoral combat ship USS *Fort Worth* (U.S. Navy/Antonio P. Turretto Ramos)

environments, and data computation and dissemination will be insufficient to satisfy future truly symbiotic human-machine system integration requirements.

Advances in machine cognition technology as well as greater understanding of human intelligence require rethinking current joint functions, particularly command and control (C2). This comes with the acceptance that machine cognition will remain rudimentary in the foreseeable future with respect to traditional warfighter-identified C2 attributes such as understanding, timeliness, relevance, robustness, and simplicity. The level of autonomy should enable the flexibility and assuredness of the commander to exert control. Autonomous control system interoperability is still nascent, particularly in the area of standardized data interfaces and information exchange models.

The fundamental method to understand and distinguish between joint functions is the way capability Key System Attributes (KSAs), or characteristics of a system—manned, robotic, or autonomous—are considered essential to achieving a balanced capability requirement solution. The number of KSAs, as identified by a capability sponsor, should maintain flexibility and take into consideration reliability, safety, and trust. Notional examples of KSAs include persistence, protection, survivability, interoperability, endurance, security, sustainability, and cognition.

While KSAs are more qualitative by design, Key Performance Parameters (KPPs) are quantifiable (see the table for notional examples of autonomous weapons system KSAs and associated performance measurement). KPPs are considered critical to the development of an effective autonomous or semi-autonomous capability. The number and character of performance parameters should allow for program flexibility and, in the case of autonomous capabilities, assure human safety. Failure of a system to meet a validated KPP safety threshold will impact overall development viability by either rescinding the validation or bringing the military utility of the associated system into question. This may result in a reevaluation of the program or the associated system, leading to modification of production increments.[15]

Safety performance metrics are codified in KPPs derived from KSAs. Both are cited in the acquisition program baseline. They are measurable, testable, and verifiable in a practical and timely manner to support follow-on decisionmaking. For this discussion, the threshold value for an attribute is the maximum acceptable value considered achievable within the available technology at low to medium risk. Performance below the threshold value is not operationally effective or suitable and may not provide an improvement over current capabilities.

The following KPPs should be considered mandatory in assuring autonomous weapons system safety. Organizations assessing joint weapons system safety conformance will provide the lead joint multidisciplinary functional capabilities boards with an endorsement of the KPP in order to receive the weapons system safety endorsement.

The *force protection* KPP is applicable to all manned semi-autonomous or autonomous systems designed to enhance personnel survivability. Force protection attributes are those that contribute to the protection of personnel by preventing or mitigating hostile actions against friendly personnel, military and civilian. This KPP emphasis is on protecting system occupants or other personnel rather than protecting the system itself.

Table. Notional Performance Measurement

System Attribute: Persistence	Key Performance Parameter	Threshold	Objective
Sensor Tracking	Mission: Tracking and locating (finding, fixing, finishing) subject of interest (SOI)		
	Measure: Timely actionable dissemination of acquisition data for SOI	2 minutes	Near real time
	Conditions: Decision quality data to the tracking entity	Area denial of SOI activities	SOI tracked, disabled
System Attribute: Interoperability	**Key Performance Parameter**	**Threshold**	**Objective**
Data Dissemination and Relay Between Dissimilar Systems	Information Element: Target data		
	Measure: Dissemination of SOI biographic and physical data	10 seconds	5 seconds
	Measure: Receipt of SOI data	Line of sight (LOS)	Beyond LOS
	Measure: Latency of data	5 seconds	2 seconds
	Conditions: Tactical/geographical	Permissive environment	Nonpermissive environment

The *system survivability* KPP is applicable to manned systems and may be applicable to robotic and autonomous systems. The intent of the KPP includes reducing a system's likelihood of being engaged by kinetic or nonkinetic fires. Survivability attributes include speed, maneuverability, situational awareness, and countermeasures; reducing the system's hardening and redundancy of critical components; and allowing the system to survive an operation in a predictable, safe manner.[16]

The *net-ready* KPP is applicable to all information systems used in the control, exchange, and display of DOD data or information. The intent of the KPP is to ensure a new system's information design fits into the existing military architectures and infrastructure to the maximum extent practicable. It is applicable to many potential autonomous weapons system KSAs, particularly interoperability, modularity, and assured autonomy.

The team to secure autonomous weapons system safety comprises capability and materiel developers, testers, and operators throughout the full system life cycle to assure technical performance and operational value. Autonomous weapons system safety requirements not only in the EMD phase but also throughout the life cycle for any system enable the identification and management of hazards and associated risks during system development, testing, and sustaining engineering activities.

Conclusion

The preceding discussion illuminates the depth of autonomous weapons system safety mechanisms currently in place while giving consideration to the future. The current review processes, already laudable for inherent safety checks and balances, will continue to serve as models as both manned and autonomous systems evolve. The strategic and programmatic implications of these game-changing technologies are the emerging cornerstones of the DOD Third Offset Strategy, particularly the shift from manned to human-machine symbiosis. Other noteworthy technology informed strategy and operational planning factors are the transitions from remote to onboard cognitive control capabilities and from program-enabled to cognitive-enabled systems.

Implications to military Service investment portfolios are significant in light of institutionalizing human-machine teaming and the complexity of autonomous system development. In recent years, unmanned aircraft systems were considered more complex and thus more expensive platforms than unmanned ground vehicles.[17] Today, and for the near future, the opposite might be true. For example, U.S. Army unmanned ground systems projected to operate with a high degree of autonomy are seen to be more complex than their unmanned aircraft system counterparts. Furthermore, advanced unmanned ground vehicles for combat operations have been developmentally more challenging since they operate in a far less structured environment. As a result, more research, development, test, and evaluation are needed to assess the impact of advanced human-machine teaming design and operation.[18] This may have broad implications for planning, doctrine, and policy, particularly in autonomous weapons system legal and safety reviews supporting current and future policy for the appropriate role of autonomy and human control in the use of force.

The ultimate purpose is to ensure military utility, avert risk, preserve life, and instill safety assurance that employment of such capability will remain clearly in the hands of human control using the judgment of military commanders, consistent with defense and national policy and relevant international convention. Even though automation will be a general feature across operating environments and weapons systems, genuine autonomy in weapons will remain rare for the foreseeable future and be driven by special factors such as mission capability requirements and the tempo of particular kinds of operations.

Current lethal autonomous weapons systems present few new legal or policy issues. Many of the most frequently voiced criticisms of these systems are actually criticisms of the policy decisions and legal questions relating to projected use. The future strategic advantage of autonomous weapons systems is still conjecture.

iRobot 510 PackBot searches for explosive devices under vehicle in Djibouti (U.S. Air Force/Maria Bowman)

Although technological progress can reduce costs, increase efficiency, and create new capabilities, we should not become infatuated with new technological devices or overconfident in the ability of new technologies to solve complex problems. Most important, we must ensure that future requirements-informed policy and strategy drive technological development and that alluring new technologies do not do the opposite. **JFQ**

Notes

[1] "Department of Defense Releases Fiscal Year 2017 President's Budget Proposal," press release, February 9, 2016.

[2] Michael C. Horowitz, "The Looming Robotics Gap," *ForeignPolicy.com*, May 5, 2014, available at <http://foreignpolicy.com/2014/05/05/the-looming-robotics-gap/>.

[3] Philip Shiman, *Forging the Sword: Defense Production during the Cold War* (Champaign, IL: U.S. Army Corps of Engineers, July 1997), 53–54, 64–66.

[4] Defense Science Board, 21.

[5] *Joint Concept for Robotic and Autonomous Systems* (Washington, DC: The Joint Staff, October 19, 2016), 2.

[6] These safeguards are explained in detail in JCIDS, *Manual for the Operation of the Joint Capabilities Integration and Development Systems*, February 14, 2015, D-58.

[7] The Joint Requirements Oversight Council is the statutory council to the Chairman of the Joint Chiefs of Staff (CJCS) in his responsibility to advise the Secretary of Defense on the priorities of the requirements identified by the combatant commanders, and the extent to which the program recommendations and budget proposals of the military Services, combatant commands, and other DOD components conform to the priorities established in strategic plans and with the combatant command priorities. CJCS Instruction 5123.01G, "Charter of the Joint Requirements Oversight Council," February 12, 2015, 5.

[8] Ibid., A-12–14.

[9] The Capability Development Document (CDD) proposes the development of a specific materiel capability solution intended to wholly or partially satisfy validated capability requirements and close or mitigate associated capability gaps. The CDD provides development Key Performance Parameters, Key System Attributes, and additional performance attributes to guide the development of one or more increments of a specific system. Each increment described by a CDD must provide a safe, operationally effective, suitable, and useful capability solution in the intended environment. See JCIDS, *Manual for the Operation of the Joint Capabilities Integration and Development Systems.*

[10] DOD Instruction 5000.69, "DOD Joint Services Weapon and Laser System Safety Review Processes," November 9, 2011, 8, available at <www.dtic.mil/whs/directives/corres/pdf/500069p.pdf>.

[11] DOD Directive 5000.01, "The Defense Acquisition System," November 20, 2007, available at <www.dtic.mil/whs/directives/corres/pdf/500001p.pdf>; and Military Standard (MIL-STD) 882E, "Department of Defense Standard Practice: System Safety," May 11, 2012, 9, available at <www.system-safety.org/Documents/MIL-STD-882E.pdf>.

[12] MIL-STD 882E.

[13] DOD Directive 2060.1, "Implementation of, and Compliance with, Arms Control Agreements," January 9, 2001, 2, available at <www.dtic.mil/whs/directives/corres/pdf/206001p.pdf>.

[14] DOD Directive 5000.01, 7.

[15] JCIDS, *Manual for the Operation of the Joint Capabilities Integration and Development Systems*, D-A-5–11.

[16] Ibid., D-A-2.

[17] John Gordon IV et al., *Comparing U.S. Army Systems with Foreign Counterparts* (Santa Monica, CA: RAND, 2015), 102, available at <www.rand.org/pubs/research_reports/RR716.html>.

[18] Ibid.