Naval War College Review

Volume 71
Number 3 *Summer*

Article 6

2018

Lifting the Fog of Targeting: "Autonomous Weapons" and Human Control through the Lens of Military Targeting

Merel A.C. Ekelhof

LIFTING THE FOG OF TARGETING

"Autonomous Weapons" and Human Control through the Lens of Military Targeting

Merel A. C. Ekelhof

Autonomous weapon systems (AWSs) have generated one of the most heated recent debates about the laws of war and military ethics. The issue of autonomous weapons flows from the concern that human beings will lose control over the weapons they use, and hence no longer will be deciding matters of life and death. Consequently, most states, participants (e.g., elements of civil society), and commentators agree that autonomous weapons require some level of human control. Different terms are introduced to reflect the premise that humans should control or interact with the autonomous system; *meaningful human control, appropriate levels of human judgment,* and *intelligent partnership* are examples of this general concept. But there is no agreement on what these concepts mean, or what exactly should be subject to this control: the weapon itself, its critical functions, or each individual attack.[1]

This article argues that, to gain a better understanding of what the concept of meaningful human control (by whatever name) means in a context of increasingly autonomous weapons, we should focus our attention first and foremost on what should be considered *targeting*. Military targeting practices within which this human control is, or ought to be, exercised should be the core of any analysis. The context within which these systems are used and human control is exercised is essential to determining what human-machine relationship we require, now and potentially in the future. Therefore, the article discusses

Merel A. C. Ekelhof holds an LLM in the law and politics of international security from and is a PhD candidate at VU University Amsterdam. She is a visiting researcher at the Harvard Law School Program on International Law and Armed Conflict and a research fellow of the Centre for the Politics of Transnational Law. Her research—commissioned by the Netherlands Ministries of Defense and Foreign Affairs—examines the effect of increasingly autonomous technologies on military decision-making.

Naval War College Review, Summer 2018, Vol. 71, No. 3

autonomous weapons through the lens of military targeting—more specifically, the targeting process.

There seems to be a considerable lack of knowledge and understanding about targeting among individual members of the public, as well as many groups that represent the public in some way, such as lawyers, nongovernmental organizations, political leaders, industry, scientists, and the press. This lack of knowledge about targeting is reflected in the discourse on autonomous weapons—which is where it becomes particularly precarious, because of repeated calls to regulate and limit military practices.[2] Although not all individuals engaging in the discourse on autonomous weapons need to understand targeting to the degree that military professionals should, the discourse would benefit profoundly from a more informed discussion regarding targeting practices, as this would provide insight into how the implementation of autonomous technologies will impact targeting decisions and human control.

This article will demonstrate that negotiating and exercising control occurs throughout the entire targeting process, and that introducing autonomous technologies into the process could lead to a loss of human control but does not inevitably do so. The manner in which a concept such as *meaningful human control* is interpreted depends on the context within which it is or ought to be applied; thus, how does the targeting process inform our discussion about control?

Answering that question requires first gaining a better understanding of what targeting is and what it is not. The first section of the article discusses the six-phase decision-making cycle that has developed over the course of history and has become embedded in the training for and execution of NATO (i.e., mostly Western) military operations; Western militaries refer to this as the *targeting process*.[3]

The second section of the article discusses one phase of the targeting process—phase 2: target development—in more detail. This detailed analysis serves two purposes: (1) It demonstrates the complexity of the targeting process, including the different layers of decision-making involved; while target selection may seem to be a straightforward task, it requires much more deliberate planning than a game of Whac-A-Mole, in which one simply attacks anything one considers a target. (2) It reconsiders what qualifies as a *critical function* of targeting. In the discourse on AWSs, critical functions are related to the weapon itself, and mostly are described as those that require human control in their execution, owing to their importance for targeting (i.e., their causal relationship to kinetic effects, and thus to potential death and destruction). Yet I argue that a critical function such as target selection is considered during multiple phases of the targeting process and need not have any direct connection to weapons use or kinetic action.[4] Therefore, instead of focusing discussions on autonomous *weapons*—the

dominant approach of the past decade or so—we ought to be focusing on autonomous *targeting*.

Thus, the third section of the article addresses the development of autonomous technologies—not weapons (although practically any technology can be weaponized)—in the targeting process. There already are many ongoing military projects in the field of artificial intelligence (AI), machine learning, autonomy, and automation that can provide case studies on how these technologies affect the processes in which they operate and how that relates to human control.[5] These developments appear to arise, first and foremost, within the intelligence branches of militaries, because of the massive increase in (and demand for) intelligence, in both quantity and quality, and because rapidly changing battle spaces demand accelerated decision-making. Although intelligence often is considered targeting *support,* it arguably can be said that intelligence personnel perform approximately 85 to 90 percent of targeting.[6] Thus, the role of intelligence and the development and use of autonomous technologies for targeting will be discussed together in the third part of the article to determine how these technologies affect human control in the process and what challenges we can identify already.

The article's final section draws some tentative conclusions about how my approach informs the debate on human control. Autonomous technologies should not be conceived as replacements for humans; rather, their introduction to the targeting process changes the tasks and activities of human actors. On the one hand, humans might be able to increase their control, instead of losing it, owing to improved situational awareness and a better understanding of the operational environment. On the other hand, introducing autonomous technologies into the targeting process presents fundamental challenges, not only to military structures and the military mind-set, but most importantly to decision-making processes and the relationships between human actors and technologies in the targeting process. If these challenges are not considered carefully, the use of autonomous technologies for targeting could result in an unacceptable loss of control.

The article provides an in-depth analysis of military practices, procedures, and experiences that goes beyond that available from general, publicly accessible sources. It can be difficult for a civilian to gain access to materials concerning military targeting, owing to the obvious sensitivities concerning the subject and the resultant restrictions placed on related information. Nevertheless, I was able not only to access those documents but also to conduct field research by participating in conferences, targeting courses, and wargames; observing simulations and exercises; and conducting formal interviews and informal conversations with over fifty military practitioners. These practitioners came from different backgrounds, nationalities, command centers, and offices and represented a broad variety of experience in targeting; they included targeteers, operators,

military planners, intelligence officers, weaponeers, commanders, and legal advisers.[7] This methodology was necessary to address the matter at hand, since to comprehend targeting one must go beyond doctrine and include the experience of military specialists. It is through the prism of their experiences that we can begin to understand the complexity of targeting, current targeting practices, and contemporary targeting dilemmas—such as the control issue that autonomous technologies raise.

The article thus provides an insider's perspective, yet is suitable for public release and relevant to both civilians and military practitioners. Its purposes are, first, to contribute to contemporary debates—primarily the discourse on autonomous weapons—through a critical and honest analysis of military targeting practices in light of the demand for and development of increasingly autonomous technologies for targeting; and, second, to provide a more holistic assessment of the effect of increasingly autonomous technologies on the human role within the targeting process, and the challenge of safely implementing these technologies while preserving human control.

TARGETING AS A PROCESS, NOT AN ACTION

Historically, *targeting* could be described essentially as the practice of destroying enemy forces and equipment. Classic targeting mainly focused on achieving victory through military kinetic lethal actions that were related directly to an enemy's military wherewithal. Targeting was primarily a tactical exercise, a process that was executed predominantly on the battlefield.

Examples of this interpretation of targeting still appear in daily news reports. Popular news sources such as Al Jazeera, CNN, the BBC, and Reuters regularly publish headlines such as "Netanyahu: Strikes in Syria Targeted Hezbollah Arms," "Air Strike on Mosque near Aleppo in Syria Kills 42: Monitor," and "U.S.: 'Jihadi John' Targeted in Drone Strike."[8] For many, when confronted with awful images of bloodshed, the urge to point the finger too frequently triumphs over the need for a more measured, considered analysis of what actually occurred.[9] Although it is difficult to generalize about the international media, such publications seem to adopt the historical approach to targeting, which focuses primarily on the effect of an attack. This tells us very little about contemporary targeting.

Arguably, targeting—in the contemporary meaning of the concept—did not evolve until the introduction of airpower in World War I.[10] Today, targeting—after a long evolutionary process and enabled by technological developments—has developed into a practice that aims to achieve specified effects on and beyond the battlefield by means of not only classic kinetic lethal actions (e.g., employing bombs, guns, torpedoes) but also nonmilitary, nonkinetic, and nonlethal activities (e.g., financial effects, electronic warfare, psychological warfare, and

information operations; the Russian interference in the American election arguably could fall within this definition).[11] No longer did targeting aim to achieve effects on the battlefield only; it became increasingly important to achieve effects in all domains and on all levels—the strategic, operational, and tactical. Nowadays, it would be more appropriate to describe targeting as a decision-making cycle that is deliberate, not ad hoc; iterative; and methodical in planning actions against adversary targets to achieve the effects needed to meet strategic and operational campaign objectives.[12] This effects-based approach, with a particular focus on linking strategic-, operational-, and tactical-level effects, also is reflected in military doctrine, some of which is publicly accessible.[13]

In the following paragraphs this doctrine will be explored further, for two main reasons. First, if we continue to consider targeting according to the historical interpretation—as an isolated tactical act—rather than as a deliberate process, we will not be able to address effectively the control issue that technological innovation raises. Second, this "helicopter view" of the process is necessary to contextualize the next part of this article, which zooms in on phase 2 of the targeting process to give a detailed analysis of the different considerations, tasks, and decisions that are made within this phase. It should provide well-grounded knowledge on how Western militaries currently exercise human control in the process within which, ultimately, increasingly autonomous technologies already are or will be employed.

One of the most significant documents on targeting—a cornerstone in NATO targeting operations—is the NATO publication *Allied Joint Doctrine for Joint Targeting,* AJP-3.9. It provides a framework of principles, practices, and procedures, the clear understanding and acceptance of which are a prerequisite for NATO targeting operations.[14] The publication aims to guide NATO military forces in their actions by explaining how targeting is planned, conducted, and assessed through six phases.[15] Although aimed at guiding NATO military forces, this document also could and should be used to educate laymen, providing them with the (unclassified) information necessary to grasp sufficiently the practice of targeting.

While AJP-3.9 is the authoritative conceptual basis for joint targeting, it clearly states that "it requires judgment in application."[16] Targeting is contextual, and hence any document, doctrine, or rule book requires translation into the specific context. Much like the laws of armed conflict, this doctrine is to be interpreted by professionals to ensure careful application of its principles and procedures in the practical world. Hence, reciting the doctrine as part of this article would be of little use. To understand targeting practices, difficulties, and challenges, one must include the experience of military specialists. It is through the prism of their experiences that we can begin to understand current targeting practices—the complexity of targeting, as well as contemporary targeting dilemmas. I

will incorporate their voices as well as my own experiences gained in targeting courses, exercises, and conferences into the analysis of the targeting process in subsequent parts of this article.

AJP-3.9 defines *joint targeting* as the process that "links strategic-level direction and guidance with tactical targeting activities through the operational-level targeting cycle in a focused and systemic manner to create specific physical and psychological effects to reach military objectives and the desired end state."[17] More specifically, joint targeting can be described by the six phases involved (the number of phases can vary depending on the doctrine, but the steps are essentially the same). Together, these six phases form a cycle that may seem sequential but is, in reality, iterative and bidirectional; sometimes phases are achieved simultaneously, and they also can overlap.

Before this targeting process commences with the first phase and formal military planning is initiated, the North Atlantic Council (NAC), comprising permanent representatives of the member states, must decide that military intervention is required by issuing a NAC initiating directive.[18] Once strategic-level assessments have been made, the NAC will provide the Military Committee (the senior military authority in NATO) with political guidance, overarching military objectives, and the desired end state for a campaign, including any constraints and restraints it wishes to impose. This guidance is the framework within which military operations can take place. The political guidance from NAC incorporates diplomatic, economic, and military considerations and is often very broad and vague.[19] These political and strategic objectives and guidance include approved target sets, as well as possible priority targets called time-sensitive targets (TSTs).[20] This guidance is passed down to the joint force commander (JFC), who is responsible for the execution of the campaign.[21] Then the targeting process commences.

Phase 1: Commander's Intent, Objectives, and Guidance

The impact of the political and strategic objectives and guidance will be experienced first in phase 1. The JFC must identify clearly, at the operational level, what is to be accomplished, under what circumstances, and within what parameters, while following the political and strategic objectives and taking into consideration any constraints and restraints imposed by the NAC and, if provided, the mandate. Because the JFC derives his or her military campaign objectives from the mandate of a particular operation, the political objectives should be unambiguously clear and well-defined to facilitate the development of feasible military objectives.[22]

Once the military campaign objectives are defined, the first activity of the joint targeting process is to take these objectives, guidance (including restrictions with regard to collateral damage), and intent and further translate them into a number

of discrete operational tasks.[23] This is an iterative process conducted between the JFC and component commanders, one that allows objectives, tasks, and supporting target nominations to be developed on every level (i.e., both joint and component).[24] It ensures that each target can be traced back to clearly defined and attainable goals for military operations and, perhaps even more important, that everyone in the targeting process is aware of the objectives and guidance. But that is not always an easy task. As stated realistically in U.S. Air Force targeting doctrine, "It is easy for those caught up in the daily battle rhythm to become too focused on tactical-level details, losing sight of objectives, desired effects, or other aspects of commander's intent. When this happens, execution can devolve into blind target servicing, unguided by strategy, with little or no anticipation of enemy actions."[25]

Hence, objectives and guidance are the cornerstone of the targeting process at each level. They should be clear, concise, measurable, and attainable, driving the targeting process effectively; but they may turn out to be vague and uninformed, presenting challenges throughout the targeting process.

Phase 2: Target Development, Validation, Nomination, and Prioritization

Phase 2 covers a range of separate but related activities that go into selecting and characterizing targets, as well as building the database of knowledge about those targets. Target development can be described most accurately as having roughly five functions: target analysis, target vetting, target validation, target nomination, and target prioritization.

As mentioned previously, the NAC passes down political-strategic guidance and approved target sets to the JFC. Even though these target sets are relatively broad, it is clear that the selection of targets is controlled top down and begins even prior to the commencement of the targeting process.[26] The essence and functions of target development will be explained in more detail in the next part of this article; for now, suffice it to say that the second phase identifies eligible targets that can be influenced to achieve the JFC's objectives, and that the principal output is a joint prioritized target list.[27]

Phase 3: Capabilities Analysis

Once the actual list of targets that can be engaged has been developed, the next step is to determine the right asset with which to engage each target.[28] *Capabilities analysis* is the process of analyzing the prioritized targets and matching to them the most appropriate capabilities, lethal and nonlethal, to generate the desired physical or psychological effects.[29]

This phase has two elements that deserve further deliberation. First, capabilities analyses are sometimes referred to as *weaponeering*. Weaponeering is the process of determining the quantity of a specific type of lethal or nonlethal

means required to generate the desired effect on a given target.[30] What is the right asset (e.g., manned asset, remotely piloted asset, or standoff attack munitions) or weapon (e.g., Hellfire missiles, two-thousand-pound bombs, or nonlethal means) for engaging this target? Do we have enough of that capability? If not, is there perhaps another capability that can be substituted for it that still generates the desired effects?[31] The output of weaponeering is a recommendation of the quantity, type, and mix of lethal and nonlethal weapons needed to achieve the desired effects while avoiding unacceptable collateral damage.[32] It also can include precautions that must be taken to avoid, or at least minimize, incidental loss of civilian life, injury to civilians, and damage to civilian objects. This is the second element of phase 3, called a collateral damage estimation (CDE).

Issues related to collateral damage already may become apparent during target development, but they are considered more prominently during the capabilities analysis. CDE often is confused with weaponeering (and weaponeering with CDE). *Collateral damage* is the unintentional or incidental physical damage to noncombatants, nonmilitary objects, or the environment resulting from an attack.[33] It is estimated as part of the planning process so as to provide the commander with an estimation—not a certainty—of collateral damage to inform his or her decision prior to target engagement.[34] CDE plays a role in the proportionality assessment, as the commander will analyze whether the expected incidental civilian harm is excessive in relation to the concrete and direct military advantage anticipated.[35]

Phase 4: Commander's Decision, Force Planning, and Assignment

During this phase, targeting instructions are communicated from the operational level to the tactical level. The JFC issues a final approval of the prioritized targets and decides on matching capabilities against these targets. Consequently, the JFC assigns these targets to the different components for further planning and execution.[36]

Any relevant constraints and restraints, whether strict or lenient, that emerged during these four phases are passed on to the assigned unit.[37] Although execution is assigned to different components (referred to as "decentralized execution"), the desired objective of the campaign remains centrally controlled.

Phase 5: Mission Planning and Execution

This phase deals directly with the planning and execution of tactical activities. Now that the prioritized targets have been assigned to the various components, the detailed mission planning will be performed for the execution of operations. Tactical-level planners will take similar steps to those described for phases 1–4, but on a more detailed level. Assessments in this phase take into account operational and legal standards, including the obligation to take feasible precautions

in attack.[38] The component commander receives the prioritized targets on which he or she will be conducting further mission planning and, eventually, execution. Once the mission planning has been completed, execution can commence.

Mission execution follows a number of logical steps. This process is referred to most commonly as the F2T2EA cycle, which stands for "find, fix, track, target, engage, and assess."[39] It is during this phase that the selected lethal or nonlethal means will be used. Hence, when debating autonomous weapon systems and the critical functions of these weapons, this is the phase focused on most. Before the mission-execution phase, weapons use has been contemplated, but no weapon yet has been launched, fired, released, or used in any manner.

In the historical approach—which perceives targeting as the achievement of kinetic effects on the battlefield—focusing on this part of the process would make perfect sense. However, in contemporary targeting procedures, weapons use is far from the only critical function of targeting. Other decisions and tasks within the targeting process are particularly relevant to the discourse on autonomous weapons, and therefore warrant even more attention. Hence, after brief consideration of the final phase of the process, the next part of this article illustrates this by providing a detailed analysis of phase 2, during which target development takes place—arguably the actual critical function of target selection.

Phase 6: Combat Assessment

The assessment seeks to evaluate the effectiveness and lawfulness of executed operations and aims to guide future operations. If targeting was no more than dropping munitions on targets, then a battle damage assessment would entail little more than taking a closer look at the target to see whether the munitions exploded on the correct coordinates.

However, most of the time effects are not easy to observe; for example, the destruction of a plane as a direct effect of an attack on an airfield—as part of simultaneous attacks on all the assets of an adversary's air-defense system, aiming to, over time, degrade the legitimacy of the regime by portraying it as incapable of protecting the populace—would offer no easy assessment.[40] Although the munitions' effect can be assessed relatively easily, the change of popular attitude is unlikely to be measurable until it is reflected in the target's behavior, and even then it is extremely difficult to conduct measurements of effectiveness.[41]

For similar reasons, it also may be difficult to assess the lawfulness of the operation. Collateral damage may not always be apparent, particularly in air campaigns; it might require ground-based assessments to acquire the necessary information about the weapon's effects on the target and its surroundings.[42]

Either way, the results of these assessments feed back into phase 1 so that goals and tasks can be adjusted accordingly.

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

A DETAILED ANALYSIS OF PHASE 2 OF THE TARGETING PROCESS: TARGET DEVELOPMENT

Considering all six phases of the targeting cycle, phase 2 (target development, validation, nomination, and prioritization) is one of the more extensive phases, particularly in terms of time and resources and the involvement of different command levels. Target selection is controlled top down as the NAC passes down (from the political-strategic level to the operational level) approved target sets; targets might include ground forces and facilities, air defenses, ballistic missiles, military supplies and storage facilities, and military or political leadership.[43] Target sets even can include civilian installations, but these may be targeted only if they qualify as legitimate military targets in accordance with the law of armed conflict and relevant international law.[44]

Clearly, these target sets are still very broad; hence they require further development in phase 2 of the targeting process. As mentioned previously, phase 2 covers a range of separate but related activities that go into selecting and characterizing targets, as well as building the database of knowledge about those targets. The five functions of this phase listed earlier—target analysis, vetting, validation, nomination, and prioritization—will be discussed individually in the paragraphs below. However, the reader should keep in mind that they are closely related and in practice not easily separable.

Target Analysis

During target analysis, the most relevant targets linked to strategic and operational objectives are identified together.[45] Once the commander's guidance is received, the target system analysis (TSA) process begins.[46] The TSA is a foundational part of the target-development process, as it enables additional, more detailed stages of target development; potential targets are derived from the TSA process.[47]

TSA products are intended to provide a comprehensive and holistic assessment of an entire target system so that, ultimately, they enable planners to comprehend a target system's functions, capabilities, requirements, and vulnerabilities so they can provide recommended targeting strategies.[48] The TSA thus yields understanding of how components of the enemy system interact and how the system functions as a whole. This includes physical, logical, and complex social systems, as well as the interactions among them. The TSA approaches targets and target sets as systems (in keeping with what is known as a system-of-systems approach) to look at interdependencies and determine vulnerabilities between systems and exploitable weaknesses that, if disrupted or affected in a specific manner, will create effects that achieve the commander's objectives.[49] It, thus, looks beyond the characteristics of a single target; a target's real importance may lie in its relationship to other targets within a particular operational system.[50]

This is an incredibly challenging task that can take up many months and may require expertise that goes beyond that normally available.

Consider the task of conducting a TSA for an oil refinery. If you strike the wrong point, the effects may be devastating. For instance, kinetically attacking an oil refinery might ignite a large fire, causing additional risks to the population and damaging the refinery beyond repair. Even aside from the high risk of collateral damage, the costs of striking the refinery itself may be extensive since, essentially, "you buy what you break."[51] An alternative approach might be to strike the oil refinery using nonlethal means. Now you need not only experienced targeteers plus someone with extensive knowledge of the oil refinery you intend to strike, but also experts on nonlethal targeting (an expertise that is still relatively rare in NATO).

In short, certain targets require more time and expertise to plan for than others. But in any case, TSA is a lengthy process that can take many months, and hence should begin well in advance of operations—preferably in peacetime.[52] Therefore, strictly speaking, TSA might not be considered part of the targeting process, since the targeting process (within NATO, at least) does not commence until the NAC determines that military intervention is required and issues its guidance and objectives. According to a senior defense analyst at the Pentagon, this is far too late for a true NATO emergency such as a surprise invasion of the Baltics or Poland; as a result, NATO always will be behind the power curve unless planning can be done earlier, with approved, clear draft objectives already developed well in advance for particular scenarios.[53]

However, it is politically sensitive to conduct target system analysis on nations with which you are not currently in conflict.[54] This restricts the ability to conduct TSAs on a national—but mostly a NATO—level, impairing the preparation process from an intelligence perspective. This could mean that at the start of an operation there would be no, or very few, prepared targets to strike. As a result, forces might run out of prepared targets within the first few days or weeks after the initiation of hostilities and be forced into a mode of primarily reacting to unanticipated events. At that point, targeting could turn into a game of Whac-A-Mole. Fortunately, there are ways to conduct TSAs on an individual national level so that, once a NATO operation begins and the coalition commences the planning process, nations can contribute their information to an integrated database, although often with strict limitations. Other opportunities to enhance the planning process lie in the technological domain, which will be addressed later.

Target Vetting

Target vetting assesses whether the intelligence used to develop the target is correct and ensures that the target performs the specified function for adversaries

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

or other actors.[55] Consequently, intelligence for target development needs to be updated and refined continually, making target development an ongoing process rather than a discrete task.[56] Although this may seem a relatively easy task—a mere "checking" of the target intelligence—the importance of this task must not be underestimated. As previously explained, target analysis can take a long time. It is therefore important to vet all the targets before they can be nominated for engagement. Not doing so could lead to inadvertent engagements and violations of the laws of armed conflict.

Target Validation

Target validation ensures that the vetted targets are in line with the JFC's objectives and desired effects, that they are in compliance with relevant international law and policy, and that the all-source analysis used to develop the targets is accurate and credible.[57] During the process of target validation, certain questions are asked. Does the target meet the JFC's objectives, guidance, and intent? Is the target consistent with the laws of armed conflict and the rules of engagement? Is the desired effect on the target consistent with the desired end state? Is the target politically or culturally sensitive? What are the risks and likely consequences of collateral damage? What are the consequences of *not* attacking the target?[58]

Finally, during target validation targets also are coordinated and deconflicted with other operations. Coordination with many other agencies and activities may be necessary to prevent friendly-fire accidents, collateral damage, or propaganda leverage for the enemy.[59] Coordinating operations, integrating joint fires, and ensuring deconfliction are all parts of a complex process, especially in a coalition in which national caveats, rules of engagement, a low tolerance for collateral damage, political constraints, and various legal issues must be taken into consideration on a multinational level. This is not even to mention the challenges that arise out of the collaboration among and organization of numerous actors from different military branches and services, and in joint operations from different nations, resulting in a conglomeration of cultural, organizational, educational, and linguistic differences.

Target Nomination

Once potential targets are validated, they are nominated by components (air, land, maritime, and special ops) for approval via the joint coordination process and identified to be included and prioritized within the joint target list (JTL).[60] The JTL is the master list from which all other lists are produced; the joint prioritized target list (JPTL), restricted target list, and no-strike list are all subsets of the JTL. The JTL provides all known targets within the NAC-approved target sets considered for engagement. That does not mean, however, that all targets on

the JTL are already selected for engagement; they still need to be cleared against the rules of engagement, NATO caveats, and relevant international law.[61] For example, the principle of distinction plays a vital role in this phase, to ensure that offensive action is directed only against military objectives and combatants, making a clear distinction between them and civilian objects and civilians.[62]

Target Prioritization

The final clearances discussed above take place during target prioritization, of which the principal output is the JPTL. Targets on this list have been legally scrutinized, risk assessed, and validated and prioritized in line with the JFC's desired effects and guidance. Before targets are placed on the JPTL, they are presented and discussed in target working groups and boards.

The short version of this process is as follows: Targets are developed and reviewed multiple times by many different staff and different commands in the Joint Targeting Working Group. Once fully developed, these targets are presented to the Joint Targeting Coordination Board, which typically consists of functional advisers (e.g., legal, political, information-operations, and electronic-warfare advisers, as required), representatives of the different components (land, maritime, air, and special operations), national representatives, and the commander.[63] Different military representatives (e.g., the chief targeteer, legal adviser, director of operations) will provide the commander with the relevant information. In the end, the commander will decide whether to approve the presented targets and place them on the JPTL, or disapprove or suspend them (e.g., owing to a lack of intelligence). The JPTL includes the proposed means of prosecution (lethal or nonlethal) and the components responsible for engaging the targets (including recommendations covering intelligence collection and additional weapons restrictions relating to collateral damage estimation analysis).[64]

Because targets and the environment within which they are located change continually and because military planners never will know everything there is to know about a target or a target solution, target development is an ongoing process. The process takes time: to enable proper planning and to perform course checks, legal reviews, proper target vetting, and more.[65] An experienced targeting professional comments, "More time has not always equated to greater success, but nearly any U.S. or NATO targeting planner would see it as a significant plus."[66]

As important as time, or perhaps even more important, is the intelligence that supports target planning; the indispensable role of intelligence and the importance of time deserve separate attention. As part of that discussion, the paragraphs below elaborate on autonomous technologies for targeting, with a specific focus on the intelligence branch and its role in target development.

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

AUTONOMOUS TECHNOLOGIES FOR TARGETING

Although autonomous *weapons* have sparked serious debates about human control over the past five to ten years, autonomous *technologies*—some of which are even weaponized—have been part of military processes for much longer. They range from simple algorithms that support calculations to complex autonomous technology that is used in modern unmanned combat aircraft (not to be confused with "regular" remotely piloted aircraft systems, commonly known as *drones*).

An illustration of the former is the Capability Analysis Tool, an automated weaponeering system that provides the standard automated methodology for estimating the employment effectiveness of most nonnuclear, kinetic weapons.[67] Another example is the software program called DCiDE, which is used for estimating collateral damage.[68] Examples of an application of complex autonomous technology in military systems are the American X47-B and the comparable British system called Taranis, the Russian MiG Skat, the European nEUROn, and the Chinese Anjian. These are unmanned combat air systems that can autonomously perform complex tasks, such as taking off from and landing on an aircraft carrier, conducting midflight refueling, and taking evasive maneuvers. Some of these systems are said to be capable of automatically identifying and targeting a threat as well, after which the system will send the data back to a human operator to be verified and to (dis)approve the engagement.[69] Autonomous behavior is inherent in many defensive responses, such as defensive cyber autonomy and defensive countermeasures in airplanes. Examples include aviation electronic systems that respond immediately to jamming indications, up to and including the deployment of defensive countermeasures, such as releasing chaff and flares, with the aircrew only flicking a "consent" switch at the beginning of the mission.[70] Additionally, defensive systems that can operate in a fully automated mode to engage preprogrammed threats such as incoming missiles already have existed for decades. Examples include the American Phalanx close-in weapon system and well-known defensive ground systems, such as the surface-to-air Patriot missile battery and the Israeli Iron Dome; all can autonomously perform their own search, detect, evaluation, track, engage, and kill assessment functions to defend ships or ground areas against fast-moving and highly maneuverable threats.[71]

However, in circumstances of self-defense, no elaborate targeting process is used to engage the target. There is reduced planning time and fewer policy constraints. Therefore, situations of self-defense are not an adequate reflection of targeting, and hence autonomous systems that are used for self-defense are not included in this analysis. The scope of this article is limited to the tasks and decisions that are made within the targeting process and are or could be considered critical functions of targeting. Consequently, the previously mentioned unmanned combat air vehicles that can autonomously perform tasks that generally

are considered less critical (e.g., those that relate to flight or navigation) also will not feature in the analysis that follows.[72]

Examples exist of both complex and relatively simple technologies that play a role in the targeting process. Sometimes these technologies are called *automated* or *autonomous;* sometimes they are described as *learning,* or as representing some other form of *artificial intelligence.* Interpretational issues are at the heart of this debate. The meanings of these technological and sometimes even philosophical terms are far from settled; they can have diverging meanings within different disciplines and in different contexts, and most of them are just inherently complex.[73] I am under no impression that this semantic dispute can and should be solved here and now. Therefore, I will refer to all these technologies (irrespective of whether they are considered automated, learning, autonomous, or some other form of AI) as *autonomous technologies*. Regardless of what type of technologies are already existent or under development, the principal concern should be to consider these technologies within the decision-making processes within which they will be used; how we as humans decide to deal with these technologies is more important than debates about the technologies themselves. In the paragraphs that follow, for each technological development discussed, the relevant context of targeting will be clarified so the impact of the technology can be assessed within an analysis of the process by which it will be used.

The Indispensable Role of Intelligence

Intelligence plays a role in each phase of the targeting process. In some, intelligence takes the lead (e.g., target development); some phases involve a mix of intelligence and operations (e.g., weaponeering); and in others the intelligence role is one of true support (e.g., force planning and assignment or monitoring tasks).[74]

Most often, intelligence is described as providing targeting support. This is a correct statement; however, it does not do justice to the real value that intelligence provides to the targeting process. Generally, the most important role of intelligence in targeting is to provide commanders and their staffs with analysis of key aspects of the operational environment to assist them in their decision-making process.[75] As mentioned above, although this role may seem merely "supportive," some estimate that targeting is 85 to 90 percent an intelligence job.[76] Irrespective of whether these percentages accurately reflect the actual role of the intelligence branch, it is clear that intelligence plays a vital, continuous, and often decisive role in the targeting process.

The value of intelligence has been an ever-present subject in military discussions. Sun Tzu wrote that if you know the enemy and know yourself, in a hundred battles you will never be defeated.[77] George Washington agreed: "The necessity of procuring good intelligence is apparent and need not be further argued."[78]

Throughout history, no one indeed has seemed to argue the point, although Clausewitz was somewhat critical, writing, "Many intelligence reports in war are contradictory; even more are false, and most are uncertain."[79] From these observations it can be concluded that intelligence is of great importance, but good-quality intelligence can be hard to come by. In addition, having more intelligence at one's disposal does not guarantee strategic success. The quality of intelligence matters at least as much as the quantity.[80]

About fifteen years ago "[w]e moved from 'Industrial age' to 'Information age' targeting . . . as the combination of new aircraft that could carry large numbers of smaller precision-guided weapons, better and more multi-source intelligence, and the ability to pass dynamic target updates from multiple sensors to airborne aircraft in minutes vastly increased the number of targets that could be struck on a given mission," says Lieutenant General John N. T. "Jack" Shanahan, Director for Defense Intelligence (Warfighter Support) at the Office of the Under Secretary of Defense for Intelligence.[81] The transformation to the information age implied, and became manifested in, information becoming the driving factor in warfare.[82] The advent of unmanned vehicles carrying improved sensors not only increased transparency on the battlefield but also enhanced the precision of weapons systems and the speed of command by compressing the time to complete decision-making loops.[83]

This capability increased the demand for intelligence for targeting, while concurrently the use of these unmanned platforms vastly increased the amount of data produced. When this was combined with increases in other types of data—most significantly, the data from open sources such as the Internet—analysts began to be overwhelmed by the constant flow of vast amounts of data, which made it impossible for them to analyze it all and convert it into information and intelligence.[84] Simultaneously, battle spaces are changing rapidly and contested areas demand accelerated decision-making—now, and likely even more so in the future.

Practice has taught us that, whether referring to NATO as a whole or to individual member states, current targeting enterprises are not prepared to handle the demands of future conflicts, beyond perhaps a counterterrorism or contingency operation that is limited in both scope and scale. NATO member states learned in the Balkans in the late 1990s, in Libya in 2011, and again at the beginning of Operation INHERENT RESOLVE that it is far too easy to overestimate targeting capacity, and as a result to run out of prepared targets to hit within days or at most weeks of commencing an operation. To bring NATO's targeting capacity up to speed and solve the multiple challenges the organization is facing today, nations cannot simply throw more people at the problem. Although having more and more-experienced personnel would definitely improve targeting, it will not

be nearly sufficient. As General Shanahan explains, "The reality is that the supply will never equal the demand. Not now. And definitely not five years from now."[85] The U.S. Joint Chiefs of Staff also acknowledged this in *Joint Vision 2010,* which explained that "instead of relying on massed forces . . . , we will achieve massed effects in other ways. Information superiority and advances in technology will enable us to achieve the desired effects."[86]

So if human personnel—even assuming they have the requisite expertise—are not expected to be sufficient to solve the problem, autonomous technology becomes a major driver. This has caused militaries worldwide to invest in these technologies for military purposes.[87]

Artificial Intelligence for Intelligence

Militaries recognize that, among other benefits in both the intelligence and operations fields, technology enables commanders and their staffs to access—sometimes in near-real time—large amounts of intelligence about the operational environment, which can assist them in planning, deciding on, and executing an attack effectively and in accordance with the relevant law and policy. The technology also enables analysts to convert raw data into actionable intelligence that can be used for targeting. Hence, intelligence is of the greatest value when humans and technology join forces. In this information age, the intelligence branch seems to be one of the first military disciplines to experience the effects of this technology on both the quantity and quality of its work—both positively and negatively.

Although the massive increase in data available might seem a positive development, the positive results remain limited if the data cannot be processed for use. With over 1.8 billion images captured on mobile phones daily, we can speak of a real data explosion.[88] Last year, Cisco (a company that provides Internet traffic forecasts) presented a white paper claiming that "[i]t would take an individual more than 5 million years to watch the amount of video that will cross global IP [Internet protocol] networks each month in 2020. Every second, nearly a million minutes of video content will cross the network by 2020."[89] This estimate covers all IP traffic, not just the data relevant to military operations; even so, open sources are becoming an increasingly relevant data source in modern operations. Furthermore, information overload is also experienced through other intelligence sources that are strictly military. For example, the amount of full-motion video (FMV) produced by unmanned aerial vehicles (UAVs) has risen sharply over the past ten to fifteen years. The amount of footage from 2008 already would take a single human being—who never slept or blinked—twenty-four years to watch.[90] Analysis of all this material is performed by hundreds of young military personnel, mostly Air Force airmen at present, but increasingly soldiers, sailors,

and Marines who view each video as it comes in.[91] Yet even then only a small amount of the data (10–15 percent) can be processed.[92] The estimate of footage from 2008 already made people wonder: How long will humans be used to review these videos? Today, almost a decade later, very little about this manual process has changed, even though technology has continued to evolve, thereby amassing more and more data—without assisting in the processing, exploiting, and disseminating thereof. Presently, monitoring, messaging, and reporting on one FMV feed from a single UAV takes a minimum of three military technicians (not counting additional personnel for supervision, maintenance, and the like).[93] This is a strenuous, labor-intensive effort that would be more effective if supported by technology.

This is one of the reasons the U.S. Department of Defense (DoD) established the Algorithmic Warfare Cross-Functional Team (AWCFT), also known as Project Maven. The overall aim of this team is to accelerate DoD's integration of AI, big data, and machine learning across operations to maintain advantages over increasingly capable adversaries.[94] Its first task is to field technology to automate processing, exploitation, and dissemination (PED) for theater- and tactical-level UAVs collecting FMV in support of the Defeat-ISIS campaign.[95] Currently, analysts spend 80 percent of their time doing mundane administrative tasks associated with staring at FMV (e.g., look, count, characterize) and typing data manually into a spreadsheet.[96] Although it is necessary to conduct such tasks, commanders and Pentagon leaders do not consider them a good use of their analysts' time.[97] So instead, they are introducing autonomous intelligence processing to help reduce the burden on the human analysts, augment actionable intelligence, and enhance military decision-making.[98] An example would be technology that can identify relevant activity and then label the data. It is a small portion of what General Shanahan—the man tasked with finding the new technology—expects the project will be able to accomplish in the future, but it is a first step that is necessary to demonstrate the utility of AI for targeting.[99] "You have to go after a manageable problem, solve it, show early wins and then start to open Pandora's box and go after all of these other challenges across the department," says Shanahan.[100]

One of the main challenges that could be tackled next is the automation of TSAs.[101] As mentioned previously, conducting TSAs is a very critical task—potential targets are derived from them—but it is also very complex and time-consuming. Target systems such as air-defense forces, lines of communication, enemy leadership, and ideology exist and operate within a complex system-of-systems context having numerous interrelationships and dependencies that may not be readily apparent, may require analysis of large amounts of data, and may not conform to preconceived notions and biases.[102] TSA therefore requires thorough analysis of a broad variety of intelligence sources and rigorous objectivity

to reveal vulnerabilities in one seemingly unrelated system.[103] In addition, this needs to be a continuous process to enable adjustment to dynamic circumstances. This is even more difficult when combating insurgents; for example, a hospital may be used as a command center, but a week later the command center may have moved and the local population may have begun to reinhabit the facility.[104]

Thus, TSA constitutes a substantial task—and with the limited number of targeteers that Western armed forces, particularly NATO, have now, it is almost impossible to perform. This would be even more problematic in a scenario in which NATO was at war against a near-peer opponent. As stated previously, states cannot bring NATO's targeting capacity up to speed and solve the multiple challenges the organization faces today simply by throwing more people at the problem. Autonomous technology, however, could speed up the process, processing large amounts of data so as to discern interrelationships and dependencies that human beings would fail to recognize. Additionally, AI is expected to play a vital role in planning; it would make it possible to run hundreds, or even millions, of simulation exercises to understand the potential effects of actions against targets across a given network.[105]

Because the TSA process not only entails the objective assessment of data for generic target system analysis but also recommends targeting strategies tied to the commander's objectives and guidance, any autonomous technology conducting this process would have to be capable of performing complex assessments or assisting a targeteer in doing so. So far, no such military technology is in use, but the importance of TSA for target development, and targeting more broadly, and the many ways in which autonomous technologies could support the process mean that TSA is an area that soon could see demands for, or even application of, autonomous technologies.

A different, but similar, project of the U.S. Intelligence Community focuses on finding mobile missile launchers, then flagging them for analysts anytime they transition from a benign to a threatening posture. Basically, this means that the program must be taught what "normal" looks like to be able to flag the difference. According to former U.S. Deputy Secretary of Defense Robert Work, this type of automation could prove most beneficial at the National Geospatial-Intelligence Agency (NGA), which gathers images from America's satellites, analyzes them, and feeds the information to the military and the Intelligence Community for targeting and other purposes.[106] The NGA also deals with datasets so large and complex that they are difficult to process using traditional data-processing applications (so-called big data). To conduct tasks such as making maps, knowing the environment, and navigating the planet, as well as understanding activity, threats, and changes, the NGA too is exploring technological solutions. For example, the NGA is developing a software program that can

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

determine a geolocation from a picture that was taken of the area of interest. This technology would enable faster searches of the data to determine a subject's location.[107] In practice, this could mean that a social-media picture of an area in which, say, a missile launcher is identified could be used to search through massive amounts of data to determine the location of the launcher within minutes (depending on the search box).

These types of technologies are often neglected in the discourse on autonomous weapons owing to the fact that they are not weaponized.[108] However, to disregard such technologies would be to ignore their potential. These technologies will be vital for target development; in particular, they will be closely connected to target selection, since the actionable intelligence produced by the human-machine collaboration very well could result in targets being selected for engagement on the battlefield. These technologies are designed to give the military a better understanding of what is happening on the battlefield, helping humans to react more quickly than their adversaries, thus giving them a better chance to win a war—or, better yet, to deter an enemy from attacking at all.[109] Automating decisions that have a direct causal link to weapons release might be most sensitive—authorizing machines to kill humans is "a bridge too far" for most political and military leaders—but technologies that can have a substantial effect on which specific targets end up on the approved target list or technologies that determine what data humans see and how they should conceive the battlefield can be just as influential, potentially even more so.

Consider the effect of autonomous technologies that decide, out of large amounts of data, what specific data to show to their operators and what data to ignore, thereby influencing or shaping situational awareness. Another consideration relevant to assessing human control in the targeting process would be the effect of data labeling on target selection. What labels are being applied (e.g., *weapon, attack, combatant, hostile intent*)? And how is this information presented to the human; is there a risk of either automation bias toward or mistrust of the system? One step further would be for target-support systems to suggest specific targets for engagement. Although a human being still would make the final decision to approve or disapprove a proposed attack, the role that autonomous technologies would have in target selection no longer can be ignored.

More importantly, if we fail to consider these types of technologies for intelligence tasks and the manner in which they are implemented within the military architecture, we risk losing a valuable opportunity to examine potential ways to manage them. A lot is being said about what the fight looks like now and what it will look like in the future, but too little time is being spent on the middle piece—the actual steps necessary to get there.[110] The aforementioned projects constitute such steps; they are the first attempts at integrating autonomous technologies

into existing military architectures and processes—specifically the targeting process. It is vital that we learn from these first attempts, understand the challenges they raise, and anticipate the ramifications thereof, because the next steps certainly will seek ways to expand the use of such technology into areas beyond intelligence.[111]

THE CONTROL ISSUE—NOW AND IN FUTURE TARGETING

In view of the targeting process and surveying current developments in the field of autonomous technologies for targeting, a few main tentative conclusions about the control issue can be drawn. These conclusions relate to implementing and incorporating autonomous technologies in (1) the military mind-set, (2) military structures, and (3) decision-making processes. These areas of concern are expected to be collectively relevant to solving the control issue.

However, as this article focuses on the targeting *process,* the next part of this analysis will focus primarily on the effect of implementing autonomous technologies into that process. But before beginning this concluding analysis, let me briefly address the challenges that arise out of implementing autonomous technologies into the military mind-set and the military structure.

Changing the Military Mind-Set

The military is well-known for its focus on hardware such as aircraft, satellites, missiles, and other platforms and munitions. But advanced software technologies are becoming more and more crucial to the success of today's military. As a U.S. Air Force general explains it, "The B-52 lived and died on the quality of its sheet metal. Today our aircraft will live or die on the quality of our software."[112]

Currently, there is a wealth of potential innovation in the commercial sector that the military (at least Western, particularly U.S., armed forces) finds difficult to identify and introduce into the defense system.[113] If military services want to take advantage of technological developments in the commercial field, they will need to be fast and agile in identifying and incorporating emerging technologies, as these commercial developments will be equally exploitable by many other states and nonstate actors. This is a challenge for an institution that takes a slow and deliberate approach to the acquisition and fielding of technologies.[114] Furthermore, there is a need for militaries to change from having a hardware mind-set—a platform-centric innovation and acquisition process—to being software-minded and understanding the potential contributions and risks that autonomy and AI can bring to military missions.[115]

This will require a fundamental change in mind-set, one that will be most difficult to achieve; military historian Basil H. Liddell Hart famously observed that "the only thing harder than getting a new idea into the military mind is to

get an old one out."[116] Even though the military's mission likely will never be fully compatible with the commercial culture—which defense analyst Peter Singer describes as "fast, flat in structure, and happy to fail and fail rapidly"—the ability of militaries to take risks and adapt will prove critical to retaining a military edge in this new environment.[117]

Dealing with the Military Structure

Transitioning from a hardware mind-set to a software mind-set will require some significant changes to the military structure, as any step in the process would need to be implemented across military branches to promote interoperability and effectiveness. However, military organizations often are very "stovepiped" and disjointed in structure. By way of illustration, a Pentagon official from the Joint Staff Targeting Division explained that when DoD acquires new software it generally is not compatible with the existing system.[118] Continuing, he noted that every geographical combatant command (known as CENTCOM, EUCOM, AFRICOM, etc.) has different architectures and can be developing tools to improve these architectures independently.[119] Thus, different developments are occurring at different commands and within different services because they use different base systems that are not compatible with another service's or command's systems.[120]

According to Dr. Bernadette Johnson of the Defense Innovation Unit Experimental, "Part of our problem is a legacy problem of the historical foundation of our independent services, and if we were a fresh brand-new country standing up today then we wouldn't design the military in the way that we currently have it."[121] Clearly, this existing military structure makes implementing new technologies across the board and achieving interoperability difficult.[122]

The Effect on Human Control in the Targeting Process

The third area of concern—but the primary one of this article—that should be considered when implementing autonomous technologies is the process within which these technologies operate. Current discussions focus on autonomous weapons and ignore the type of autonomous technologies that this article discusses. One of the reasons for this exclusive and narrow focus on weapons and the platforms that carry them seems to be that, like intelligence, these autonomous technologies are considered to have "supporting" functions, implying that they support but do not replace a human decision. As a result, it is expected that a human being remains accountable for any violations of the applicable law, policy, or military ethics.[123] Also, the level of risk in the event that the technology makes a mistake is considered to be lower because the human will act as the ultimate decision maker.

Nevertheless, it should be noted that even if these technologies are playing a supporting role, and even if a human being ultimately makes the decisions,

the technologies can influence critical targeting decisions—which could be both positive and negative. On the one hand, autonomous technologies could be beneficial, for example, in terms of speeding up the process and processing large amounts of data to discern interrelationships and dependencies that human beings would fail to recognize. Western armed forces are struggling to keep their targeting capacity up to speed, and the complexity, scope, and scale of the targeting process mean that mistakes happen. Autonomous technologies provide opportunities to improve this process and its results. On the other hand, implementing these technologies in the targeting process gives rise to additional and new challenges with regard to human-machine interfaces, (incompatible) ethical frameworks, trust issues, training, and more. These are all fundamental discussions that influence the manner in which the control issue is perceived. Although solving all of them is beyond the scope of this article, some operational effects can be identified that are relevant from a human-control perspective.

With the targeting process as the reference framework, one could conclude that an effect of using increasingly autonomous technologies for targeting is that human actors and technologies are becoming part of a long chain within which decisions made by one link in the chain almost definitely will affect the control or limit the decisions of others in the chain.[124] In short, implementing autonomous technologies will affect the control that human actors further down the chain (i.e., within the targeting process) can exercise. This could result in a shift of responsibilities that, for example, might generate an increase in responsibilities for certain superiors or the developers of systems, but also could result in a lack of accountability if the effects of implementing these technologies are not considered adequately before the technologies are introduced into the process. (This issue is also closely related to the military structure.)

Even without autonomous technologies, the targeting process is an inherently complex process within which many individuals make numerous decisions on a daily basis. Hence, responsibility for critical decisions typically is spread across the entire process. On the one hand, this provides multiple opportunities to exercise control and apply checks and balances. On the other hand, it should be no surprise that such complex processes—within which a conglomeration of cultural, organizational, educational, and linguistic differences are at play—are prone to human errors. Mistakes are made; the question is whether autonomous technologies can reduce these mistakes or ultimately will cause more, or perhaps different, mistakes.[125]

Furthermore, it should be noted that the use of autonomous technologies *changes the activities* of human actors; such technologies do not simply *supplant* the human beings, who simultaneously relinquish all the responsibilities and

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

control they exercised previously.[126] To the contrary, the proper use of autonomous technologies may lead to improved situational awareness and a better understanding of the operational environment that may even enable human beings to enhance their control. Nevertheless, this is not without risk; the redistribution of existing tasks and the creation of new ones change the relationship between human actors and technologies, which can give rise to a transformation in decision-making processes.[127] If these transformations are not considered thoroughly, the use of autonomous technologies could ultimately result in an unacceptable loss of human control. Whether humans remain in control of critical targeting decisions depends on how well they succeed at creating a framework within which this control can continue to be exercised alongside the use of increasingly autonomous technologies.

So far, no state has addressed these concerns comprehensively and effectively. However, some first attempts at creating a framework can be observed on the current political landscape, where a significant number of states seem to be open to prescribing self-imposed restrictions on the development and use of autonomous weapons, with specific reference to human control.[128] In fact, some states already have gone one step further and implemented certain requirements in their national policies. The U.S. DoD, for instance, published a policy that directs that "autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[129] And according to the Netherlands, "meaningful human control is required in the deployment of autonomous weapon systems."[130] Even though the number of such government policies currently is small—most governments merely commit to official statements or working papers presented in expert meetings held under the UN Convention on Certain Conventional Weapons (CCW)—the majority of these policies or statements include a reference to the relevance of human control.

Hence, nations seem committed to keeping human beings in the decision-making loop for important targeting decisions—at least for now. However, it could very well be that, if a major conflict arises, all bets will be off, with states feeling forced into more reliance on autonomous systems because their adversaries are willing to take more risk.[131] Considering warfare's historical action-reaction cycle, algorithm-versus-algorithm warfare between two adversaries may not be too far off.[132]

However, this is not an inevitable result of these technologies; rather, it is a choice that human beings make if they decide to introduce these technologies into the targeting process without considering—or after deliberately accepting—the

consequences. In the current situation and for Western armed forces, this is not likely to be a deliberate choice, but it very well could be the result of a misunderstanding of the issue that leads to an erroneous method of dealing with these new technologies. For example, by focusing merely on weaponized technologies, states, participants, and commentators fail to take into account other significant phases of the targeting process and the technologies that affect critical targeting decisions in other ways. What they do not seem to realize is that focusing solely on weapons employment is like assembling a jigsaw puzzle while staring only at one corner—through a soda straw.

Therefore, this article advises taking an expansive view, considering the targeting process as a reference framework under which to examine holistically the effect of autonomous technologies on human control. While doing so, governments could learn from current projects that aim to implement autonomous technologies in targeting, such as Project Maven.

They also should consider learning from previous experiences with implementing new technologies in the targeting process. For example, the Center for Naval Analyses (CNA) concluded in its report on mitigating civilian casualties resulting from the use of drones that "[f]ailure to recognize and mitigate factors besides the platform in the targeting process resulted in an increased risk to civilians from the use of drones, despite some desirable characteristics of those systems."[133] Research into operational data from U.S. drone missions in Pakistan and Afghanistan confirmed that "reducing civilian casualties depends on the entire engagement process, including planning and training considerations, not simply on characteristics of the weapon platform."[134] Although the platforms under discussion in this article are not the same, much of the decision-making process is. Hence, these assessments could help states understand the changing dynamics in the targeting process caused or exacerbated by the introduction of new technologies.

To conclude, the reality is that autonomous technologies already are and will continue to be important for targeting. Therefore, safely incorporating these technologies into targeting is not a concern for the future but a challenge that should be addressed today rather than tomorrow. States that claim that human control or judgment is essential to making proper targeting decisions often simultaneously pursue autonomous technologies, claiming that these technologies represent the future of targeting. It could be concluded from this article that one approach does not need to preclude the other, but we ought to be mindful of the effects that autonomous technologies will have on our decision-making processes.

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

The development and use of autonomous weapons have created a host of legal, political, and ethical questions and concerns that continue to be scrutinized, primarily within the CCW process. However, the annual deliberations that are held under this framework convention have resulted in little progress over the past four years. Nonetheless, so far over two dozen states have endorsed the notion of "meaningful human control" or a similar concept that ought to prevent humans from losing control over autonomous weapons. Yet how the concept should be interpreted and applied remains vague and disputed.

This article has argued that the principal concern should be to consider these autonomous technologies within the decision-making processes in which they will be used, because that is the primary context within which their effects can be assessed properly. The reference framework that I propose is the targeting process. Yet there appears to be a considerable lack of knowledge about targeting among many groups and individuals, many considering it to be merely the practice of destroying enemy forces and equipment. This historical approach is no longer suitable for describing contemporary targeting.

Today, targeting should be perceived as a deliberate, analytical, and iterative process, rather than an isolated tactical action. It aims to achieve specified effects on and beyond the battlefield by means of not only classic kinetic lethal actions but also nonmilitary, nonkinetic, and nonlethal activities.

This process begins on a political-strategic level, at which military intervention is decided on and political guidance and overarching military objectives are formulated. This guidance is passed down to the operational level, at which time the targeting process commences. Through the six phases that follow, military forces formulate operational objectives, select and prioritize targets, match them with the appropriate response, consider operational requirements and capabilities, execute the mission, and assess whether the desired effects were achieved.

The targeting process provides an appropriate and holistic framework to consider concepts such as "meaningful human control" or "appropriate levels of human judgment." Human control and judgment are exercised within this process, and hence the targeting process should be considered in its entirety to determine the effect of increasingly autonomous technologies on human control. Also, inquiry should not be limited to weapons deployment but expanded to the entire targeting process; such an expansive view demonstrates that critical targeting decisions are made throughout the process, so the scope of the control issue exceeds the mere use of autonomous weapons. In this context, the detailed analysis of phase 2, target development, not only demonstrates the complexity of the targeting process; it moreover confirms that critical targeting functions need have no direct relation to weapons or kinetic action. It also redirects attention

to the targeting role of a military branch—intelligence—that largely has been ignored in the debate on autonomous weapons.

With the advent of the information age, the intelligence branch appears to be one of the first military disciplines to experience the effects of technology on both the quantity and quality of its work, both positively and negatively. Western armed forces cannot deal with the targeting challenges they face simply by throwing more people at them, so states are driven to invest in technological solutions. The U.S. DoD's AWCFT—tasked with integrating AI, big data, and machine learning across operations—provides an example. One of its first efforts has been to automate intelligence processing to reduce the burden on human analysts, augment actionable intelligence, and enhance military decision-making. This is only one of many ongoing research and development projects that Western states—and most certainly many others—are pursuing.[135]

Nevertheless, these types of technologies often are neglected in the discourse on autonomous weapons because they are not weaponized. This article establishes that disregarding these technologies is a mistake. First, these autonomous technologies used for target development have an effect on which specific targets end up on the approved target list by determining what data humans see and how they should conceive the battlefield. The fact that these technologies are not weaponized is irrelevant, as their tasks are potentially even more critical for targeting than those of their weaponized cousins. Second, these projects provide an opportunity to examine challenges and potential ways of dealing with the implementation of increasingly autonomous technologies in the targeting process.

A closer look identifies three main challenges. First, as advanced software technologies become more and more crucial to the success of today's military—assuming the various services want to take advantage of these technological developments—militaries need to change from a hardware to a software mindset, since the ability of militaries to take risks and adapt will prove critical for retaining an edge in this new environment. Second, the military structure is very stovepiped and disjointed, making it difficult to implement new technologies across the board. Third, implementing autonomous technologies in the military targeting process will be a task of significant difficulty. Even without autonomous technologies, the targeting process is an inherently complex process within which many individuals make numerous decisions on a daily basis, inescapably resulting in mistakes.

Although imperfect, the targeting process serves as a reliable basis on which to analyze the effect of increasingly autonomous technologies, work toward better protection of civilians, and preserve military effectiveness. Autonomous technologies could improve this process, while, at the same time, there is a risk that

Naval War College Review, Vol. 71 [2018], No. 3, Art. 6

the use of autonomous technologies could ultimately still result in an unacceptable loss of human control because we were not sufficiently mindful of the consequences of these technologies with regard to our decision-making processes.

One effect of using increasingly autonomous technologies for targeting is that human actors and technologies are becoming part of a joint chain in which the decision of one almost certainly will affect the control or limit the decisions of others involved in the chain. Also, autonomous technologies change the activities of human actors; they do not supplant those actors while simultaneously relieving them of all the responsibilities and control they exercised previously. The use of autonomous technologies prompts a change in the relationship between human actors and technologies that will require a transformation in decision-making processes. If these changes and transitions are not considered properly or are ignored altogether, the use of autonomous technologies for targeting could ultimately result in a loss of human control.

So far, no state has addressed these concerns comprehensively and effectively, but some states have made initial, minor attempts at creating a framework. Such states seem to be open to prescribing informal and formal self-imposed restrictions on the development and use of autonomous weapons, with specific reference to human control. However, if a major conflict arises all such self-imposed restrictions—such as the need for meaningful human control—very well may be discarded, potentially resulting in an unacceptable loss of human control over critical targeting decisions in the targeting process.

This concern may turn out to be justified, but, as I argue in this article, this is not an inevitable result of the development and use of these technologies. Instead, whether humans remain in control of critical targeting decisions will depend on how well they succeed at creating a framework within which this control can continue to be exercised alongside the use of increasingly autonomous technologies. Even though the targeting process creates a structure that provides a basis for negotiating, exercising, and maintaining this control, we also should be honest about our targeting capacity—and the limitations thereof—and about the complexity of organizing and executing military operations—and the mistakes that result from that. Using the targeting process as a reference framework thus creates opportunities for human beings to remain in control of increasingly autonomous technologies, as long as we assess it holistically and do not ignore the complexities and challenges inherent in these complex enterprises.

NOTES

The author is very grateful to all the parties who contributed to this article, whether by commenting on drafts; allowing me to take part in courses, exercises, simulations, and conferences; or welcoming me to their offices to hear their firsthand experiences and collect the data that was indispensable to its completion.

1. The pluralistic terms and inconsistent use of terminology in the discourse on autonomous weapons often result in lengthy semantic disputes. What is meant by terms such as *autonomous, targeting, human control,* or even *weapon*? The meanings of most such terms can diverge between and within different disciplines; they often have different labels that are used interchangeably; some terms represent parts of broader concepts; and some of the concepts in question are just inherently complex. This significantly complicates the debate. Read more about the complications of a common language in Merel A. C. Ekelhof, "Complications of a Common Language: Why It Is So Hard to Talk about Autonomous Weapons," *Journal of Conflict and Security Law* 22, no. 2 (July 2017), pp. 311–31.
2. Ibid., pp. 316–17. In international discourse, most references to targeting are actually to target recognition, focusing on the ability of the autonomous weapon to differentiate combatants from noncombatants. Commonly, functions considered critical to target selection and attack relate to the weapon itself, not the more deliberate planning phases of the targeting process.
3. There are two types of targeting: *deliberate targeting* and *dynamic targeting*. This article focuses primarily on deliberate targeting, but in large part also applies to dynamic targeting. Dynamic targeting consists of the same steps, but is more responsive than deliberate targeting, since the process is used to prosecute targets that are identified too late to go through the deliberate targeting process. The dynamic targeting process is compressed in time. North Atlantic Treaty Organization [hereafter NATO], *Allied Joint Doctrine for Joint Targeting,* AJP-3.9 (n.p.: NATO Standardization Office, 2015), p. 2-4. With regard to autonomous technologies, dynamic targeting raises some distinct issues that fall outside the scope of this article but may be addressed in a later piece.
4. In 2016, the International Committee of the Red Cross (ICRC) introduced *critical functions* as a concept to describe the challenges that autonomous weapons raise, and states, participants, and commentators have used the concept since then. The ICRC refers to critical functions in relation to the weapon itself. ICRC, *Autonomous Weapon Systems: Implication of Increasing Autonomy in the Critical Functions of Weapons* (Versoix, Switz.: Expert Meeting, 2016).
5. Examples include the Algorithmic Warfare Cross-Functional Team (Project Maven); research into military autonomy at the Netherlands Organization for Applied Scientific Research (TNO); scouting by the Defense Innovation Unit Experimental (DIUx) for emerging technologies; many commercial projects that are relevant to the military, such as learning algorithms used by Facebook and Google; and National Geospatial-Intelligence Agency research into geolocation software. Earlier investigations into fratricide with automated weapon systems, such as the U.S. Army and Navy investigations into the Patriot shoot-down of a Navy F-18 in Iraq in 2003, continue to be relevant. Larry Lewis, *Operation Iraqi Freedom: Ground-to-Air Fratricide,* CNA Research Memorandum D0008910.A4 (CNA, July 2004).
6. Intelligence operations specialist in the office of the Under Secretary of Defense for Intelligence at the Pentagon, interview by author, May 18, 2017.
7. The information in this article was cleared for public release by the Netherlands Ministry of Defense. The personal information of the interviewees remains confidential; however, an overview of the different command centers and offices that were consulted during this research can be provided on request.
8. "Netanyahu: Strikes in Syria Targeted Hezbollah Arms," *Al Jazeera,* March 18, 2017, www.aljazeera.com/; Angus McDowall and Idrees Ali, "Air Strike on Mosque near Aleppo in Syria Kills 42: Monitor," *Reuters,* March 16, 2017, www.reuters.com/; Jim Sciutto, "U.S.: 'Jihadi John' Targeted in Drone Strike," *CNN,* November 13, 2015, edition.cnn.com/.

9. William H. Boothby, preface to *The Law of Targeting* (Oxford, U.K.: Oxford Univ. Press, 2012).
10. Frans P. B. Osinga and Mark P. Roorda, "From Douhet to Drones, Air Warfare, and the Evolution of Targeting," in *Targeting: The Challenges of Modern Warfare,* ed. Paul A. L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga (The Hague, Neth.: T. M. C. Asser, 2016), p. 29.
11. Paul A. L. Ducheine, Michael M. Schmitt, and Frans P. B. Osinga, introduction to *Targeting,* ed. Ducheine, Schmitt, and Osinga, p. 1.
12. U.S. Air Force, "Dynamic Targeting," in *Annex 3-60 Targeting* (Montgomery, AL: Curtis E. LeMay Center, 2017), p. 7. As explained in note 3, this article focuses on deliberate targeting and does not discuss dynamic targeting specifically. There are strong similarities between the two types of targeting, although dynamic targeting often is considered more ad hoc in nature because the targets in question are identified too late to be included in the deliberate targeting cycle.
13. See, for example, U.S. Air Force, *Annex 3-0 Operations and Planning* (Montgomery, AL: Curtis E. LeMay Center, 2016), p. 13.
14. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-4.
15. Ibid., p. vii.
16. Ibid.
17. Ibid., p. 1-1.
18. A request for the development of an operational plan will follow by Supreme Headquarters Allied Powers Europe, known as SHAPE—prepared at the level of the JFC and adjusted and approved by the NAC—after which the NAC issues a NAC execution directive and the targeting process can commence. Targeting experts, interview by author, February 22, 2017.
19. See, for example, S.C. Res. 1973, Libya (March 17, 2011), and Chris De Cock, "Targeting in Coalition Operations," in *Targeting,* ed. Ducheine, Schmitt, and Osinga, pp. 238–39.
20. A TST is a target that requires immediate response because it poses (or soon will pose) a danger to friendly forces or is a highly lucrative, fleeting target of opportunity. TSTs are of such high priority that their effective engagement can make or break the campaign, so the JFC is willing to divert assets away from other targets to find, fix, track, target, engage, and assess them. NATO, *Allied Joint Doctrine for Joint Targeting,* p. Lexicon-9.
21. These objectives and guidance are passed down from the NAC to the JFC, through the Military Committee and Strategic Command. Ibid., p. 3-1.
22. De Cock, "Targeting in Coalition Operations," p. 238.
23. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-3.
24. Ibid.
25. U.S. Air Force, *Annex 3-60 Targeting,* p. 42.
26. Mark Roorda, "NATO's Targeting Process: Ensuring Human Control over (and Lawful Use of) 'Autonomous' Weapons," in *Autonomous Systems: Issues for Defence Policymakers,* ed. Andrew P. Williams and Paul D. Scharre (Norfolk, VA: Headquarters Supreme Allied Commander Transformation, 2015), p. 155.
27. NATO, *Allied Joint Doctrine for Joint Targeting,* pp. 2-3–2-4.
28. Targeting expert, interview by author, December 1, 2016.
29. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-4.
30. U.S. Air Force, *Annex 3-60 Targeting,* p. 70.
31. Targeting expert interview.
32. U.S. Air Force, *Annex 3-60 Targeting,* p. 70.
33. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 1-10.
34. Thus, collateral damage issues are considered not only in phase 3 but also in phase 1 (commander's objectives and guidance), phase 2 (target development), and phase 5 (mission planning and execution), and therefore are a good example of considerations that play a role in different phases.
35. No attack is to be launched that is expected to cause collateral damage excessive to the concrete and direct military advantage anticipated. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 51(5)(b) and 57(2)(a)(iii), June 8, 1977.

36. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-4.
37. Roorda, "NATO's Targeting Process," p. 159.
38. Precautionary measures include doing everything feasible to ensure the target is a lawful military target; taking all feasible precautions in the choice of means and methods of attack, with a view to avoid or minimize collateral damage; canceling or suspending an attack if it becomes apparent that the target is not a lawful military objective or the attack will be disproportionate; and giving effective warning, if the circumstances permit. Protocol Additional art. 57; Roorda, "NATO's Targeting Process," p. 160.
39. This cycle also is used to describe dynamic targeting. It applies even to the deliberate process because operations, by their nature, are dynamic.
40. U.S. Joint Forces Command, *Commander's Handbook for Joint Battle Damage Assessment* (Suffolk, VA: Joint Warfighting Center, 2004), p. I-8.
41. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-7.
42. Larry Lewis, *Drone Strikes in Pakistan: Reasons to Assess Civilian Casualties* (Arlington, VA: CNA, 2014), pp. 17–20.
43. Some of these can be targeted both kinetically and nonkinetically, while others, such as political leadership, can be targeted only nonkinetically. NATO, *Allied Joint Doctrine for Joint Targeting,* p. B-1.
44. Ibid. If the JFC wishes to appoint targets from categories that are not included in the NAC-approved target sets, the JFC has to seek approval.
45. Ibid., p. 2-3.
46. Joint Chiefs of Staff, *Target Development Standards,* CJCSI 3370.01 2011 (Washington, DC: Office of the Chairman, 2011), p. C-4. Besides the TSA process, there is also a target audience analysis (TAA). TAA is defined as follows: "The systematic study of people to enhance understanding and identify accessibility, vulnerability, and susceptibility to behavioral and attitudinal influence activity." Rita LePage and Steve Tatham, *NATO Strategic Communication: More to Be Done?* (Riga: National Defense Academy of Latvia, 2014), p. 10.
47. Joint Chiefs of Staff, *Target Development Standards,* p. B-10.
48. Ibid., p. C-2.
49. A target system most often is considered as a collection of assets directed to perform a specific function or series of functions. U.S. Air Force, *Annex 3-60 Targeting,* pp. 7, 11, 61.
50. Ibid., p. 11.
51. Experienced targeteer, interview by author, during NATO exercise, February 2017.
52. U.S. Air Force, *Annex 3-60 Targeting,* pp. 35, 61.
53. Intelligence operations specialist interview.
54. John N. T. "Jack" Shanahan [Lt. Gen.], interview by author, May 17, 2017; targeting experts interview.
55. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-3.
56. Target development begins in phase 2 after receipt of the commander's objectives and end state, but it continues in phase 3 (capabilities analysis), phase 4 (force planning and assignment), and phase 6 (assessment). The focus on continual target development in these phases should ensure that the most current and accurate target intelligence is part of the commander's decision process. Joint Chiefs of Staff, *Target Development Standards,* p. B-6.
57. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-4.
58. U.S. Air Force, *Annex 3-60 Targeting,* p. 63.
59. Ibid., pp. 63–64.
60. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 2-4.
61. Ibid., p. 4-7.
62. Ibid.; Protocol Additional arts. 48, 51–52.
63. NATO, *Allied Joint Doctrine for Joint Targeting,* p. 4-6.
64. Ibid., p. 4-7.
65. Phillip R. Pratzner, "The Current Targeting Process," in *Targeting,* ed. Ducheine, Schmitt, and Osinga, p. 82.
66. Ibid.
67. Joint Chiefs of Staff, *Joint Targeting,* JP 3-60 (Washington, DC: Office of the Chairman, 2013), p. B-3.

68. Joint Targeting School, "Collateral Damage Estimation Course Syllabus," October 2015, available at www.dtic.mil/.
69. Frank Slijper, *Where to Draw the Line: Increasing Autonomy in Weapon Systems—Technology and Trends* (Utrecht, Neth.: PAX, 2017), p. 10, available at www.paxvoorvrede.nl/.
70. John N. T. "Jack" Shanahan [Lt. Gen.], e-mail to author, December 30, 2017.
71. Ekelhof, "Complications of a Common Language," p. 2.
72. Military transformation has been a U.S.-led process that, among other aspects, has centered on the exploitation of new information technologies. Therefore, the examples and descriptions of developments in the field of autonomous technologies that feature in this analysis primarily reflect U.S. projects and procedures. European states simply have been unable to match the American level of invest ment in new military technologies. Chinese and Russian developments are not included in the analysis owing to a lack of sufficient reliable sources. Theo Farrell and Terry Terriff, "Military Transformation in NATO: A Framework for Analysis," in *A Transformation Gap? American Innovations and European Military Change,* ed. Terry Terriff, Frans Osinga, and Theo Farrell (Stanford, CA: Stanford Univ. Press, 2010), p. 1.
73. Ekelhof, "Complications of a Common Language," p. 13.
74. Targeting expert interview.
75. Joint Chiefs of Staff, *Joint Intelligence,* JP 2-0 (Washington, DC: Office of the Chairman, 2013), p. I-27.
76. Intelligence operations specialist interview.
77. Sun Tzu, *The Art of War,* ed. and trans. Lionel Giles (New York: Race Point, 2017), p. 12.
78. John Keegan, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda* (Sydney: Random House, 2010), p. 9.
79. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton Univ. Press, 1976), p. 117.
80. The Vietnam War was instructive for the United States in this respect, as the 2006 Israel-Hezbollah war was for Israel. Pratzner, "The Current Targeting Process," p. 83.
81. John N. T. "Jack" Shanahan [Lt. Gen.], "The Future of Targeting" (paper presented at the NATO ACO Targeting Conference, Strasbourg, Fr., February 7, 2017). Also see Osinga and Roorda, "From Douhet to Drones," pp. 43–44.
82. Frans P. B. Osinga, *Science Strategy and War: The Strategic Theory of John Boyd* (New York: Routledge, 2007), p. 245.
83. Ibid.
84. *Intelligence* is not the same as *information* or *data*. When *data* are collected and processed into an intelligible form, the end result is *information*. Information can be of utility to the commander, but when related to other information about the operational environment and considered in the light of past experience, it gives rise to a new understanding of the information, which may be termed *intelligence*. Joint Chiefs of Staff, *Joint Intelligence,* p. I-1.
85. Shanahan, "The Future of Targeting."
86. Joint Chiefs of Staff, *Joint Vision 2010: America's Military; Preparing for Tomorrow,* p. 17, available at webapp1.dlib.indiana.edu/. Also see Frans Osinga, "The Rise of Military Transformation," in *A Transformation Gap?,* ed. Terriff, Osinga, and Farrell, p. 24.
87. See, for example, the U.S. Third Offset Strategy, the Chinese national-level AI development plan, and Russia's political response to these developments and continuing discussions. Robert O. Work [Deputy Secretary of Defense], "Third Offset Strategy" (remarks, Brussels, April 28, 2016), available at www.defense.gov/; Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," *Center for a New American Security,* November 28, 2017, www.cnas.org/; Patrick Tucker, "Russia to the United Nations: Don't Try to Stop Us from Building Killer Robots," *Defense One,* November 21, 2017, www.defenseone.com/.
88. Technical director and big-data specialist at the NGA, interview by author, May 16, 2017.
89. "Cisco Visual Networking Index: Forecast and Methodology, 2015–2020," *Cisco,* 2016, p. 3, www.cisco.com/.
90. Aaron Saenz, "US Military Drowning in Drone Data," *Singularity Hub,* January 22, 2010, singularityhub.com/.

91. Ibid.
92. Shanahan interview.
93. Ibid.
94. U.S. Deputy Secretary of Defense, memorandum, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," April 26, 2017, available at www.govexec.com/.
95. Intelligence, surveillance, and reconnaissance (ISR) PED specialist and AWCFT manager at the Pentagon, interview by author, May 15, 2017.
96. Marcus Weisgerber, "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS," *Defense One,* May 14, 2017, www.defenseone.com/.
97. Ibid.
98. U.S. Deputy Secretary of Defense, memorandum, "Establishment of an Algorithmic Warfare Cross-Functional Team."
99. Shanahan interview.
100. Weisgerber, "The Pentagon's New Algorithmic Warfare Cell."
101. Shanahan interview.
102. Joint Chiefs of Staff, *Target Development Standards,* p. B-6.
103. Ibid.
104. Targeting experts interview.
105. Shanahan e-mail.
106. Marcus Weisgerber, "The Increasingly Automated Hunt for Mobile Missile Launchers," *Defense One,* April 28, 2016, www.defenseone.com/.
107. NGA technical director and big-data specialist interview.
108. The CCW (discussed below) is an umbrella agreement that discusses prohibitions or restrictions on the use of certain conventional weapons, not certain technologies. Thus its focus on weapons makes sense. However, to address the specific challenges that the technologies might raise, one needs a different approach.
109. Colin Clark, "The War Algorithm: The Pentagon's Bet on the Future of War," *Breaking Defense,* May 31, 2017, breakingdefense.com/.
110. Pentagon official from the ISR division, e-mail to author, July 20, 2017.
111. Weisgerber, "The Pentagon's New Algorithmic Warfare Cell."
112. Christian Hagen, Steven Hurt, and Jeff Sorenson, "Effective Approaches for Delivering Affordable Military Software," *CrossTalk* (November/December 2013), p. 26.
113. Jesse Ellman, Lisa Samp, and Gabriel Coll, *Assessing the Third Offset Strategy* (Washington, DC: Center for Strategic and International Studies, 2017), p. 6. In past years, the U.S. DoD responded to this difficulty by creating several new organizations to address those deficiencies and meet current and projected operational needs. Examples are the Strategic Capabilities Office, the DIUx, and the previously mentioned AWCFT. Larry Lewis, *Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations* (Washington, DC: CNA, 2017), pp. 10–20.
114. Lewis, *Insights for the Third Offset,* p. 8.
115. U.S. Air Force software specialist, interview by author, May 18, 2017; ISR PED specialist and AWCFT manager interview; senior intelligence officer at U.S. DoD Joint Staff Targeting, interview by author, May 17, 2017.
116. B. H. Liddell Hart, *Thoughts on War* (London: Faber & Faber, 1944).
117. Jeremy Hsu, "Despite Trump, Silicon Valley's Pentagon Ties Stay Strong," *Wired,* February 10, 2017, www.wired.com/; Lewis, *Insights for the Third Offset,* p. 8.
118. Senior intelligence officer interview.
119. Ibid. See also Lewis, *Insights for the Third Offset,* p. 26.
120. Senior intelligence officer interview; Lewis, *Insights for the Third Offset,* p. 26.
121. Bernadette Johnson, remarks for "Innovation and the Future Force" panel discussion (Center for a New American Security, May 17, 2017, Washington, DC), video available at www.cnas.org/.
122. Lewis, *Insights for the Third Offset,* p. 22.
123. For an assessment on distributed responsibility within the context of the military chain of command, see Marcus Schulzke, "Autonomous Weapons and Distributed Responsibility," *Philosophy and Technology* 26, no. 2 (June 2012).

124. On responsibility practices and unmanned systems, see Merel Noorman, "Responsibility Practices and Unmanned Military Technologies," *Science and Engineering Ethics* 20, no. 3 (September 2014), pp. 809–26.

125. It is relevant to note here that there is an important difference between discussing which human-machine relationship would be most beneficial for achieving a desired goal (i.e., how AI can improve the targeting process) and determining what we would consider ethically acceptable.

126. The effects of their introduction into the targeting process will vary, but the understanding that autonomous technologies are not simply human replacements could be illustrated by the introduction of UAVs. Although often perceived as taking the pilot out of the cockpit, the actual effect of UAVs has been much more significant than that. Armed UAVs still need a substantial crew, including the pilot, a sensor operator, a mission-intelligence coordinator, and several analysts to deal with tasks at hand. In fact, it can take up to 168 people—including operators; coordinators; advisers; analysts; crews for landing, takeoff, and flight; technicians; and maintenance personnel—to keep a Predator in the air for twenty-four hours. Noorman, "Responsibility Practices and Unmanned Military Technologies," p. 818.

127. Ibid., p. 817.

128. This mostly refers to statements made during the Convention on Certain Conventional Weapons 2013–16 expert meetings on lethal AWSs, during which a majority of states pointed out—frequently—the need for some form of human control. See Ekelhof, "Complications of a Common Language."

129. U.S. Defense Dept., *Autonomy in Weapon Systems,* Directive 3000.09 (Washington, DC: November 21, 2012), p. 2.

130. Government of the Netherlands, "Government Response to AIV/CAVV Advisory Report No. 97, 'Autonomous Weapon Systems: The Need for Meaningful Human Control,'" March 2, 2016, available at aiv-advies.nl/.

131. Shanahan interview.

132. Shanahan e-mail.

133. Lewis, *Drone Strikes in Pakistan,* pp. 1–2.

134. Ibid., p. 28.

135. See note 72 for a methodological clarification of the author's primary Western/U.S. focus.