Issue 41

October 2020

Legal Gazette

Legal Aspects of Innovation

Contents

***Introduction**, by Sherrod Lewis Bumgardner*..... **4**

- **Preface**, *by Geoffrey S. Corn and Gary Corn*..... **6**
- **Innovation for peaceful purposes only: Where there is the will, there is ITER**, *by Antoaneta Boeva* **14**
- **Partnership, Not Pivot: NATO's Legal Answer to the China Question**, *by Lauren Brown* **27**
- **Responsibility, Liability and Lethal Autonomous Weapon Systems**, *by Theodora Vassilika Ogden* **46**
- **Autonomous Weapon Systems: A Pragmatic Approach to an Emerging Capability**, *by Major Gregg F. Curley*..... **61**
- **U.S. Export Controls: The Future of Disruptive Technologies**, *by Christopher Timura, Judith Alison Lee, R.L. Pratt and Scott Toussaint* **96**
- ***The Relevance and Benefits of Integrated Compliance Strategy (ICS) for NATO Defence Forces**, by Martijn Antzoulatos-Borgstein* **125**
- ***Legal Operations: The Use of Law as an Instrument of Power in the Context of Hybrid Threats and Strategic Competition**, by Rodrigo Vázquez Benítez*..... **138**
- ***The Road to Hell is Paved with Bad Contractors: Vendor Vetting is a Better Path**, by Brett Sander* **145**

Publisher:
Monte DeBoer, ACT Legal Advisor

Editor-in-Chief:
Sherrod Lewis Bumgardner, ACT SEE Legal Advisor

Editors:
Mette Prassé Hartov, HQ SACT Deputy Legal Advisor
Galateia Gialitaki, ACT SEE Legal Assistant

Copy Editors:
Robert 'Butch'Bracknell, HQ SACT Staff Legal Advisor
Col Xavier Labarriere, HQ SACT Staff Legal Advisor
Miles S. Porter, HQ SACT Legal Extern
Malia Kenza Chenaoui, ACT SEE Legal Extern

Copy Proofreader:
Caitlin Fendon, HQ SACT Legal Intern
Lola Chanfreau, ACT SEE Legal Extern

Disclaimer:

The NATO Legal Gazette is produced and published by Headquarters Supreme Allied Commander Transformation (HQ SACT). The NATO Legal Gazette is not a formal NATO document and does not represent the official opinions or positions of NATO or individual nations unless specifically stated. The NATO Legal Gazette is an information and knowledge management initiative, focused on improving the understanding of complex issues and facilitating information sharing. HQ SACT does not endorse or guarantee the accuracy of its content.

All authors are responsible for their own content. Copyright to articles published in the NATO Legal Gazette may be retained by the authors or their employer with attribution to the issue of the NATO Legal Gazette the article first appeared in. Retention of the copyright an article by the author or their employer will be identified with the copyright symbol © followed by the name of the copyright holder. Any further publication, distribution, or use of all or parts from these articles are required to remain compliant with the rights of the copyright holder.

Absent specific permission, the NATO Legal Gazette cannot be sold or reproduced for commercial purposes.

Source : https://innovationhub-act.org/

Source : www.act.nato.int

Introduction

Dear Fellow Legal Professionals and Persons Interested in NATO,

This issue of the *NATO Legal Gazette* is the brain child of Robert (Butch) Bracknell who advocated using the *Gazette* to share and socialise innovative legal transformational ideas from legal advisors in academia, international organizations, commercial practice, and industry.

Issue 41 begins with a **Preface** by Geoffrey and Gary Corn, retired U.S. Army Judge Advocates and now noted academics. They consider technological changes from the 1980s to the present and incisively invite our attention to: "1) the development of the cyber domain and the adoption of cyber operations as a means and method of military and other security related operations; 2) the movement towards the development of lethal autonomous weapon systems (LAWS); and 3) the reshaping of the information environment and the attendant impact on perceptions of strategic legitimacy," knowing that "NATOs best minds must stake out the cutting edge territory of these innovations."

Antoaneta Boeva is a lawyer for the ITER Organization in Saint-Paul-lès-Durance, France. Her article, **Innovation for peaceful purposes only: Where there is the will, there is ITER** describes the remarkable engineering and legal efforts to create a star on Earth in the International Thermonuclear Experimental Reactor. Lauren Brown, an Associate in the International Trade Group of Squire Patton Boggs, a full-service global law firm, writes about the power of innovation in NATO's relationships in **Partnership, Not Pivot, NATO's Legal Answer to China.**

Theodora Vassilika Ogden, a Fellow at the Human Security Centre in London who is currently studying at Leiden University, and Gregg Curley, a Judge Advocate in the U.S. Marine Corps, accept the challenge to stake out their perspectives on LAWS and autonomous weapons. Ms. Ogden's article considers **Responsibility, Liability and Lethal Autonomous Weapon Systems** and Major Curley provides his views in **Autonomous Weapons: A Pragmatic Approach.**

Christopher Timura, Judith Alison Lee, R.L. Pratt and Scott Toussaint, who are attorneys in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and members of the firm's International Trade Practice Group provide us an important article on the interplay between industry and national security is **U.S. Export Controls: The Future of Disruptive Technologies.** Martijn Antzoulatos-Borgstein, the Trade Compliance Manager for Rockwell Automation for Europe, Middle East and Africa, follows by proposing collective actions by NATO and partner nations to better manage the industry-security interplay in **The Relevance and Benefits of Integrated Compliance Strategy (ICS) for NATO Defence Forces.**

Rodrigo Vázquez Benítez is an Assistant Legal Advisor in the Allied Command Operations Office of Legal Affairs at the NATO Supreme Headquarters Allied Powers Europe. He addresses the reshaping of the information environment by providing a description of the exploitation of the legal domain in a context of strategic competition in **Legal Operations: The Use of Law as an Instrument of Power in the Context of Hybrid Threats and Strategic Competition.**

Brett Sander, a US legal practitioner and principal at Vendor Clearance LLC, provides our final thoughtful article, **The Road to Hell is Paved with Bad Contractors: Vendor Vetting is a Better Path.**

The contributions of Butch and each of the accomplished authors of the nine articles in Issue 41 is deeply appreciated and you, the readers, are thanked for your interest in the *NATO Legal Gazette*.

Best wishes to you all from Belgium.

Lewis
Sherrod Lewis Bumgardner
Legal Advisor
ACT Staff Element Europe

Source: www.nato.int

Preface

by Geoffrey S. Corn[1] and Gary Corn[2]

When we enlisted in the 1980s to pursue our commissions as new lieutenants in the U.S. Army, the world was a very different place, but the forces of momentous change were already in motion. When I (Geoffrey) graduated Officer Candidate School (OCS) in 1984, ours was a Cold War Army, singularly focused on the doctrine of AirLand Battle designed to defeat the Soviet threat in conventional, combined arms mechanized warfare in Europe. By the time I pinned gold bars on Gary's shoulders at his OCS graduation five years later, the seeds of evolutionary, if not revolutionary change had already germinated. The Soviet Bloc had begun to unravel that same year, leading to its eventual collapse just two years hence. In the meantime, the U.S. put on stark display the power of new technologies such as stealth, GPS, and "smart bombs" in its decisive and overwhelming defeat of Iraq's armed forces in the First Gulf War. Through the three decades of our collective military experience we have witnessed profound changes in the threats our Nation, allies and partners confront, as well the fundamental character and arguably the nature of warfare itself. In many respects,

[1] Geoffrey S. Corn is The Presidential Research Professor of Law at South Texas College of Law Houston in Houston Texas. Prior to joining the South Texas College of Law Houston faculty in 2005, Professor Corn served in the U.S. Army for 21 years as an officer, and a final year as a civilian legal advisor,

[2] Gary Corn is the Director of the Technology, Law & Security Program and Adjunct Professor of Cyber and National Security Law at American University Washington College of Law; a Senior Fellow in National Security and Cybersecurity at the R Street Institute; a member of the Editorial Board of the Georgetown Journal of National Security Law and Policy, and the Founder and Principal of Jus Novus Consulting, LLC.

technology has fueled these changes, and has developed at a pace unlikely to abate in the near future. Meanwhile, states struggle to adapt their strategies and doctrine to these changes and emerging threats. While the armed forces of NATO nations must remain prepared for the "high-intensity" combat contingency, confronting and defeating non-state enemies and other unconventional "gray zone" threats is increasingly central to the missions these forces must be prepared to execute.

Technology has long been central to the evolution of the way professional armed forces conceptualize and prepare for conflict. Technological advances have always impacted war, but the nature and pace of advancements in the past several decades may very well be regarded by historians as unprecedented. It is therefore altogether fitting that the NATO Legal Gazette focuses an issue on legal aspects of this technological change.

While the impact of new technologies cuts across almost all aspects of the threat landscape and military operations, three areas of technology-driven change are worth particular note: 1) the development of the cyber domain and the adoption of cyber operations as a means and method of military and other security related operations; 2) the movement towards the development of lethal autonomous weapon systems (LAWS); and 3) the reshaping of the information environment and the attendant impact on perceptions of strategic legitimacy. How NATO and its constituent-member armed forces manage new technologies and their impacts will obviously depend in large measure on the nature and character of the technologies themselves. International and domestic law will also play a key role in framing this management process. However, one of the greatest challenges for legal regulation in the domain of emerging technology is the reality that law, especially international law, is by its very nature slow to develop and rarely proactive in nature. This means that legal advisors must often draw on rules and norms that were simply not developed in contemplation of the factual particularities presented by these new technologies.

Yet, reliance on established rules and principles also contributes to valuable predictability and stability in the regulation of military operations; or at a minimum the mitigation of regulatory chaos. These rules and principles have proven remarkably resilient in addressing the range of emerging regulatory challenges produced by emerging technologies. But there is also danger that dogmatic or formalistic adherence to legal interpretations

developed in very different contexts will undermine the ideal symmetry between technological and legal evolution.

This symmetry is essential if law is to remain relevant to those responsible for planning and executing military operations. Indeed, the resilience of the laws and customs of war writ large is a powerful testament to the wisdom of those who contributed to its development and their recognition of the requirement to strike a rational balance between competing military and humanitarian interests. Preserving this balance remains essential as the law seeks to keep pace with technology, and the perspectives of practitioners, both legal and operational, as well as technical experts and legal scholars will be essential to achieve this goal.

Consider, for example, the range of issues implicated by the development of Lethal Autonomous Weapons Systems (LAWS). From a legal perspective, questions related to the ability to comply with International Humanitarian Law (IHL) targeting principles dominates the debate over truly autonomous lethal weapon systems – systems that rely on artificial intelligence to make attack judgments with no "human in the loop." LAWS proponents emphasize the potential for artificial intelligence to make more predictable and accurate decisions than humans, resulting in enhanced compliance with these legal principles. Critics respond by questioning whether artificial intelligence will ever be capable of engaging in the type of contextual legality assessments central to compliance with these principles. Furthermore, they question whether "robotic killings" can ever be consistent with the implicit moral foundation that underlies IHL.

Operationally, the benefits of LAWS seem almost self-evident. The capacity to enhance the accuracy of target engagement while reducing the mortal risk to friendly forces should appeal to any commander. But even here questions arise. One of the most interesting is the extent to which commanders will be willing to "outsource" the exercise of human judgment to artificial intelligence. This is an especially significant consideration for the current generation of commanders and future commanders who understand that the conflicts they fight will almost inevitably endanger civilians and civilian property. These commanders also understand that legitimacy will be an increasingly significant aspect of strategic success, and hence any perception of indifference to the suffering of civilians will compromise tactical and operational effectiveness. Commanders rely on the training and development of subordinates and the human relationships between their

leadership and the teams they lead to navigate complex tactical and operational challenges. As a result, while the appetite for technology that contributes to and enhances the quality and accuracy of human judgments may be voracious, removing humans from attack judgments altogether may be perceived as inconsistent with the function of battle-command.

Commanders and other operational leaders will face profound challenges in relation to their capacity to influence the execution of attacks conducted by LAWS. While autonomy is already a feature of some weapon systems, fielding systems developed as substitutes for human cognitive reasoning central to target selection and engagement will effectively nullify a commander's ability to influence that reasoning process. Unlike the soldier who is tactical and moral reasoning is molded as a member of a coherent unit, the LAWS will arrive in the commander's arsenal with fully developed reasoning capacity. As a result, the evolution of LAWS will also require reconsideration of the doctrine of command responsibility. The vicarious liability for the foreseeable misconduct of subordinates imposed on commanders pursuant to that doctrine is premised on the expectation that commanders will discharge their responsibility to prepare the soldier to engage in hostilities consistent with fundamental legal and moral obligations and that the commander will act decisively to prevent violations when circumstances indicate they are objectively foreseeable. LAWS will undermine the symmetry between the capacity of a commander to develop and control a subordinate's reasoning skills and the liability for failing to effectively discharge this responsibility. Accordingly, it may be necessary to shift the focus of this vicarious liability from the commander to the agent responsible for validating and fielding the LAWS.

Cyber provides an even more timely example of the importance of a wide range of perspectives to inform legal evolution. In just a few short decades, the internet has exploded across the globe, transforming nearly every aspect of public and private life. Cyberspace defies geopolitical borders, is predominantly owned, operated, and managed by the private sector, resides largely outside of national control, is integrated with the operation of critical infrastructures, and forms the backbone of commerce, governance, and national security. At an increasing rate, networks and systems of military value are fully interconnected with and often dependent on cyberspace, making them potentially lucrative targets for military operations. States and non-state actors have been quick to recognize the transformative nature of cyberspace, to include the ubiquitous dependencies

and vulnerabilities inherent in its adoption and structure.

Source: www.nato.int

Seizing on these characteristics, states and non-state actors have adopted cyber operations as a means to engage in traditional, and not-so-traditional, statecraft and conflict in pursuit of their interests and to gain low-cost asymmetric advantages over their adversaries. Exploiting the many technical, policy, and legal ambiguities inherent in this nascent but now universal domain, threat actors are engaged at an increasing rate in a range of intrusive and aggressive cyber operations and activities. Unfortunately, the development of legal and policy parameters governing these operations, and states' responses thereto, have not kept pace with the rapid evolution of the environment or the threat. Attorneys charged with reviewing and advising on the legality of cyber operations are continuously called on to address difficult issues of first impression.

Unfortunately, official efforts at clarifying and evolving the normative frameworks applicable to cyber operations have been anemic and fallen short. Beyond general statements that international law applies to such operations, international bodies such as the United Nations Group of Governmental Experts (UNGGE) have made little progress in reducing legal ambiguity. To the contrary, in its final round of meetings the UNGGE retreated from the consensus it had previously achieved on the baseline proposition of international law's applicability to cyber operations. Nor have states provided much clarity individually on their views.

The legal, policy, and ethical challenges attendant to the growing reality of cyber operations are profound. These non-kinetic operations do not neatly square with extant definitions and understandings of those military actions such as "attacks" that lie at the heart of Law of Armed Conflict (LOAC) regulation, and risk undermining core principles such as distinction and precautions when conducted, per force, within the predominantly civilian domain of cyberspace. Properly understanding and characterizing the impacts of in bello cyber operations will be critical to ensuring adherence to and advancement of the LOAC consistent with its object and purpose. And as states and non-state actors continue to leverage cyberspace to

engage in aggressive "gray zone" operations, the underdeveloped legal landscape will only become more apparent.

Yet it is beyond dispute that states are bound by international law, to include in the conduct of cyber operations, and ambiguity as to the specifics of application in no way relieves commanders or the lawyers advising them of this obligation. In the absence of official state positions, the importance of the growing body of academic literature and the work of unofficial commentaries and compendiums such as the first and second Tallinn Manuals on the International Law Applicable to Cyber Operations cannot be understated. Providing fora such as this issue of the NATO Legal Gazette for the presentment of differing perspectives on these important issues is essential for development of the law generally, and to aid legal advisors in the formulation of legal and policy advice.

Emerging technologies, most notably those that facilitate the development, manipulation, and diffusion of information, have profoundly changed the information environment within which states must conduct military and other security operations, facilitating the weaponization of information and amplifying its impact on perceptions of strategic legitimacy in unprecedented ways. Commanders and the forces they lead operate in a world where real-time information related to their operations can be transmitted to world-wide audiences in near real time. And, unlike prior eras, this information is increasingly unfiltered, producing a veritable cottage industry of pundits and commentators. Even more troubling is the ease by which information may be manipulated or distorted to contribute to strategic information campaigns aimed at undermining public, political, and diplomatic support for military campaigns.

This potential exploitation of the global information environment will impose increasing demands on commanders to ensure their forces are prepared to navigate the most complex tactical and operational challenges in strict compliance with all international and domestic legal obligations. It will also increase the importance of prompt and credible investigatory and disciplinary responses to allegations of misconduct. But this trend also demands more extensive efforts to educate the broader public on the space the law actually provides to military forces to accomplish their missions, and rejection of the often troubling tendency to adopt an apologetic tone for consequences of completely lawful military actions. Anything less will play into the hands of enemies who view information not as a supporting effort to

combat operations, but combat operations as a supporting effort to their information campaign. For these potential adversaries, tactical victory is never the realistic objective. Instead, the consequences of tactical action – most notably civilian casualties – are exploited to delegitimize what are in fact lawful military operations and in so doing erode the political will for their militarily superior opponents to continue the fight. This phenomenon will only increase as technology facilitates the exploitation of information, and NATO must prepare to win not only the conventional fight, but the information campaign.

Technology and the innovations it facilitates will undoubtedly reach other aspects of NATO operations as a new generation of NATO warriors seek to leverage capabilities they have grown up with to enhance effectiveness. These innovations might not as legally complicated as those associated with cyber and LAWS. However, any use of technology to influence the preparation, planning, execution, or assessment of military operations will inevitably involve legal implications. One need only imagine how technology will continue to enhance realistic combat training, enhancing the capacity of NATO forces to execute their missions in compliance with legal obligations; or how autonomy might be leveraged for humanitarian purposes, such as the fielding of robotic casualty collection platforms. Emerging technology is simply bound to reach ever military battlefield operating system and NATOs best minds must stake out the cutting edge territory of these innovations.

New technologies are, pardon the pun, nothing new. Throughout history, the advent of new technologies has evolutionized, and at times, revolutionized not just the character of warfare, but the broader interstate security environment as well. At each turn, new technologies have stressed existing legal frameworks aimed at regulating military and security operations, and at times have laid bare destabilizing lacuna in the law. The same is true today, exacerbated however by the exponentially faster rate of technological changes in the last few decades. Mindful of the singular role states play in the establishment of international law, the considered views of academics, commentators, and practitioners are essential to informing the iterative process of adapting the law to account for the changed circumstances brought on by new technologies. The thoughtful works that follow in this issue are valuable contributions to this process.

Technology and the innovations it facilitates will undoubtedly reach other aspects of NATO operations as a new generation of NATO warriors seek

to leverage capabilities they have grown up with to enhance effectiveness. These innovations might not as legally complicated as those associated with cyber and LAWS. However, any use of technology to influence the preparation, planning, execution, or assessment of military operations will inevitably involve legal implications. One need only imagine how technology will continue to enhance realistic combat training, enhancing the capacity of NATO forces to execute their missions in compliance with legal obligations; or how autonomy might be leveraged for humanitarian purposes, such as the fielding of robotic casualty collection platforms. Emerging technology is simply bound to reach ever military battlefield operating system and NATOs best minds must stake out the cutting edge territory of these innovations.

***

(20 April 2017) The seven flags of the ITER Members—and one for the ITER Organization —fly proudly over the construction site in Saint Paul-lez-Durance, France.
Source: https://www.iter.org

Innovation for peaceful purposes only: Where there is the will, there is ITER[1]

By Antoaneta BOEVA[2]

Between the Durance and Verdon Rivers in the southern region of Provence, France, is the enormous construction site[3] of the International Thermonuclear Experimental Reactor (ITER). This is the home of the ITER Organization, one of the newest international organizations. The ITER Organization came into being in 2007 when The Agreement on the Establishment of the ITER International Fusion Energy Organization for the Joint

[1] "Iter" in Latin means "the way". Originally an acronym which stood for 'International Thermonuclear Experimental Reactor', the name of the Organization was subsequently changed to ITER International Fusion Organization or "ITER Organization", as a nod to both its historic and scientific origins, but also its ambition to produce the clean and virtually unlimited energy of the Sun.

[2] Antoaneta Boeva is a lawyer at ITER Organization. The views expressed in this article are the author's only and do not necessarily reflect those of the ITER Organization, its members or their respective representatives. © 2020 ITER Organization; **ITER Organization, Route de Vinon-sur-Verdon, CS 90 046, 13067 St. Paul Lez Durance Cedex, France.**

[3] The 360° virtual tour of ITER construction has been updated with drone footage from March 2020. Fly in, out and over the principal buildings of the ITER worksite by clicking on the teardrop-shaped markers. See:< https://www.youtube.com/watch?v=IW5ELQKPPlQ>.

Implementation of the ITER Project[4] came into force.

The ITER Organization oversees a scientifically ambitious project of massive complexity and scale. The aim is to demonstrate the feasibility of fusion power as a source of safe, carbon-free, and virtually limitless energy. When completed the ITER machine will be the world's biggest nuclear fusion reactor. It will also be the only fusion reactor yielding more energy than it consumes. The ITER machine will accomplish this singular achievement by creating and controlling self-heating ("burning") plasma. The ITER Organization will then test if tritium, a rare radioactive isotope of hydrogen, can be produced during the fusion reaction, thus creating a path to energy self-sufficiency. The ITER Organization is coordinating all of the scientific, technical, legal, and political innovation at the heart of the ITER project. This paper will provide a view of each of these areas and their contribution to international cooperation and innovation for peaceful purposes.

Conceived in Geneva

The Geneva Summit, November 1985
Source: https://www.iter.org

In November 1985 --amid the thawing of the Cold War -- Geneva hosted a summit between General Secretary Gorbachev and President Reagan. One outcome of this summit—heavily focused on nuclear non-proliferation and other security issues—was an invitation for international cooperation on fusion energy. The last paragraph of the joint statement (right after the topics on preservation of the environment and education—two other issues which have today a recognized role in sustainable peace and security) declared:

Fusion Research

The two leaders emphasized the potential importance of the work aimed at utilizing controlled thermonuclear fusion for peaceful purposes and advocated the widest practicable development of international cooperation in obtaining this

[4] The Agreement on the Establishment of the ITER International Fusion Energy Organization for the Joint Implementation of the ITER Project (the "ITER Agreement") was signed on 21 November 2006 and entered into force on 24 October 2007. All articles cited in the present articles refer to the ITER Agreement.

source of energy, which is essentially inexhaustible, for the benefit of all mankind. [5]

Robert Arnoux, a long-time chronicler of the ITER Organization, marveled at the extraordinary prescience of Secretary Gorbachev's and President Reagan's call for fusion research. "It was the last item in a long list that ranged from the strategic ('a nuclear war cannot be won and must never be fought') to the trivial ('increased television coverage of sports events'). But it was an item that, in the long term, held the potential to change the course of civilization." [6]

The 1985 Gorbachev-Reagan statement laid the foundation for what has become an immensely complex and innovative scientific project; a full-blown international organization; a map of all the innovation and technologies necessary to build your own tokamak[7]; and from the perspective of a French nuclear lawyer, both a French nuclear operation with international status and an international nuclear operator on French soil. [8]

"The Project" or a "project"?

Capitalization matters, particularly in treaties. The ITER Agreement capitalizes the "ITER Project" or "the Project" twenty-two times in its thirty-two pages with the uncapitalized word "project" used just twice. The title of the treaty confirms the ITER Organization was put in place for the "joint implementation of the ITER Project" (majuscule). The Preamble reveals that "ITER" existed as a concept long before the organization, that the ITER Engineering Design Activities had been completed elsewhere, that it was time to "initiate the ITER Project", and that it required a genuine partnership for such a "long term and large-scale project" [9] (miniscule).

---

[5] Joint Soviet-United States Statement at the Summit Meeting (Reagan-Gorbachev) in Geneva, November 21, 1985. < https://undocs.org/pdf?symbol=en/A/42/669/Add.1>

[6] R. Arnoux, 'Conceived in Geneva, born in Reykjavik, baptized in Vienna' (ITER Newsline, 16 Nov 2015) <https://www.iter.org/fr/newsline/-/2323> accessed 1 May 2020.

[7] "Tokamak" is abbreviation from the Russian "*тороидальная камера с магнитными катушками*" and is a toroidal (a ring-shaped object) apparatus for producing controlled fusion reactions in hot plasma. See *Oxford Dictionaries*, Oxford University Press 2020 at https://premium.oxforddictionaries.com/definition/english/tokamak?q=Tokamak

[8] Mrs. Laetitia Grammatico is currently Head of Legal Affairs at ITER Organization. In 2009, when the work cited here was written, she was the Head Legal Advisor at the ITER-France Agency within the French Atomic Energy Commission (CEA). See L. Grammatico, 'ITER: Which Laws Apply to this International Nuclear Operator?' NEA Nuclear Law Bulletin 84, no. 2 (2009), 103-113 (DOI: 10.1787/nuclear_law-v2009-art17-en).

[9] Recital 10, "AFFIRMING the importance of genuine partnership in implementing this long term and large scale

The reason for this emphasis is because neither fusion nor fission reactors nor international cooperation concerning nuclear energy were particularly new. Fusion, which is how the Sun and stars burn, occurs when hydrogen nuclei collide, fuse into heavier helium atoms and release tremendous amounts of energy. [10] This is essentially the opposite of how standard nuclear power plants operate, as they rely on fission, resulting in the nucleus of an atom being split into two or more smaller nuclei, also releasing energy (but also quite a lot of decay). Achieving fusion requires plasma, the fourth state of matter, which occurs at extremely high temperatures and which is a tenuous environment - a million times less dense than the air we breathe - providing the environment in which light elements can fuse and yield energy. [11] By the mid-1950s fusion machines were operating in half a dozen countries around the world. In the late 1960s Soviet research produced the tokamak, the heart of which is a donut-shaped vacuum chamber which uses magnetic fields to contain and control the hot plasma, and which was capable of reaching both the required temperature levels and plasma confinement. The innovative purpose of the ITER Agreement far exceeded building another reactor. Fusion reactors—whether of the tokamak design or others—exist in many corners of the world. Many of them supply the ITER machine with blueprint or testing capabilities. [12] However, even the best reactors produce a spark which lasts only seconds. They all consume far more energy than they produce. By comparison, the Sun doing a star's work is easy: its mass allows for a self-sustaining reaction. Doing this in a laboratory requires a machine capable of supplying three conditions: very high temperature (to provoke high-energy collisions); sufficient plasma particle density (to increase the likelihood that nucleus collisions occur); and sufficient confinement time (to hold the plasma, which has a propensity to expand, within a defined volume). [13] The goal of the ITER tokamak is to achieve what scientists call a "burning plasma," one where the energy produced becomes so large that it exceeds the energy injected into heating the plasma—an achievement which has never occurred on Earth.

---

project for the purpose of fusion energy research and development;" See Preamble, ITER Agreement.

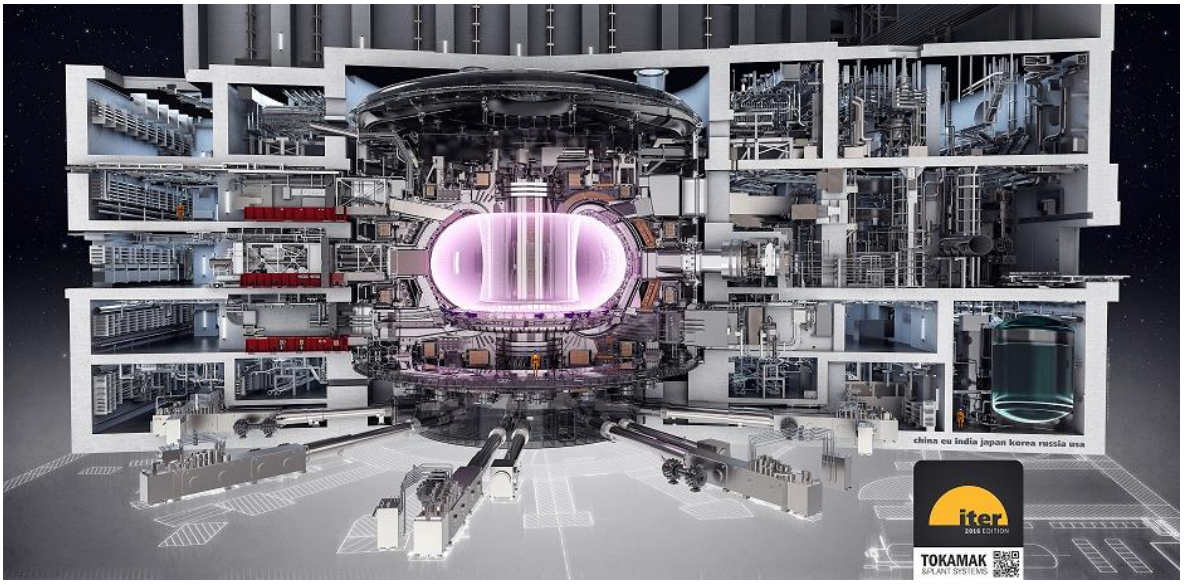
[10] Source: 'What is fusion?' https://www.iter.org/sci/whatisfusion accessed 29 April 2020

[11] Source: 'ITER: Making it work'https://www.iter.org/sci/MakingitWork accessed 29 April 2020

[12] For an overview of the world's tokamaks and their relation or contribution to the ITER tokamak, see 'International Tokamak research' https://www.iter.org/sci/tkmkresearch accessed 29 April 2020

[13] The paragraphs on the science of fusion are entirely sourced from ITER Organization series of entries explaining the science behind the Project https://www.iter.org/sci/makingitwork accessed 29 April 2020

In 1986, a year after the Gorbachev-Reagan summit, work began on what has now become, arguably, humanity's largest and most ambitious scientific project. The ITER tokamak cannot match the size and mass of the Sun. To overcome this limitation, its temperature has to be higher. Much higher: 150 million °C which is ten times higher than the temperature at the heart of the Sun. Because industrial elements cannot withstand contact with such temperatures, holding the plasma off the walls of the reactor will require superconducting magnets cooled at temperatures comparable to the coldest spots in the universe. When functional the ITER tokamak will be the hottest and (close to) the coldest places in the Universe just a few meters apart, quite a first-of-a kind endeavor for humanity.



(ITER Tokamak and plant systems, 2016) - The Tokamak and its plant systems housed in their concrete home. An estimated one million parts will be assembled in the machine alone. Source: https://www.iter.org

The ITER machine will not provide energy for commercial consumption. This will be done by another generation of tokamaks informed by the construction and operation of the ITER tokamak (and some are already in the making). They will share their energy with the power grid. [14] The ITER Organization will provide an opportunity to study burning plasmas, thus fulfilling its sole purpose: to provide a forum for cooperation "on the ITER Project, an international project that aims to demonstrate the scientific and technological feasibility of fusion energy for peaceful purposes, an essential

[14] For a peek into what's coming after ITER see "After ITER" https://www.iter.org/sci/iterandbeyond accessed 28 April 2020

feature of which would be achieving sustained fusion power generation" (Art. 2).

With the ITER Organization its Members harnessed, by political will, more than 60 years of scientific research on fusion. Proceeding in a single direction began under the auspices of the International Atomic Energy Agency (IAEA) in 1987, when the world's major fusion programs worked for two years on the ITER Conceptual Design Activities. Following this, the soon-to-become ITER Members agreed to the Engineering Design Activities (EDA) Agreement, which ran until 2001. The EDA provided the initial design of the fusion power plant, a coordinated and reasoned combination of assumptions, engineering specifications, and safety requirements. [15] With the EDA Report in hand—and the ITER Members convinced of both feasibility and requirements—"the Organization" coordinating it all could be launched. With the creation of the ITER Organization vision met execution.

The International Organization

After 2001 "the Project" needed a body more permanent than the forum provided by the IAEA; something more centralized than the teams of hundreds and thousands of scientists who had directly or indirectly contributed to the design of the ITER tokamak and plant. The Project needed proper project management. While this joint venture presented requirements, which may have pointed to an almost private partnership, other considerations had to be addressed in addition to displaying the ability and agility to efficiently allocate the final design and procurement of over a million components among the ITER Members.

For instance, the Project needed the capability to cross borders and pass customs with ease, privileges available only to certain agreed entities or persons. It also needed to ensure the full respect of the Members' sovereign positions in nuclear matters and the corresponding international fora, including export control, non-proliferation or disarmament. In sum, the Project needed an international organization with a functional status that combined independence for the Organization, and its Members, with the privileges, immunities and legal capacity necessary for accomplishing the mission.

Project blood runs through the veins of the ITER Organization. A ruling

[15] For full account of the design activities, see 'ITER Technical Basis', IAEA Documentation Series No. 24 (IAEA/ITER EDA/DS/24), IAEA, Vienna, 2002, 816 p

"Baseline" [16] details scope, schedule, cost and risks. Project management tools organize and track the design, manufacturing, testing, acceptance, assembly, commissioning and functioning of this million-parts puzzle. Yet execution by schedule and efficiency is not the only rule.

The ITER Council meets twice a year to review the most recent reports on organizational and technical performance.
Source: https://www.iter.org

Unlike a private enterprise, the ITER Members chose a work plan that ensured cooperation and would benefit everyone. The center of the ITER Project innovation—the donut-shaped tokamak—was divided like an orange. Each Member received a section that was their task to deliver. This analogy simplifies the work allocation because there are many other components and systems that are required to sustain the whole fusion power plant. Allocation is also not exactly equivalent, but the choice to share the pioneering work gave all ITER Members the opportunity for true innovation to occur everywhere. Together all could develop their research and manufacturing capabilities. All could organize their industrial supply chains. All could independently and collectively experience the responsibility of building and delivering critical components necessary for the success of the ITER Project.

The ITER Organization—a Subject of International Law

Founded by a treaty and established under international law, ITER Organization is, in most respects, a classic international (intergovernmental) organization with unique qualities. It has its own legal personality, privileges, immunities and a mostly standard governance structure. Its youth is perhaps the reason behind some more modern aspects of its structure and governance. For instance, Euratom, the sole remaining entity of the European Communities[17], is a founding member of the Organization. ITER Organization

[16] See 'ITER Council endorses updated project schedule' (ITER Newsline, 21 Nov 2016) https://www.iter.org/newsline/-/2588

[17] The three entities originally composing the European Communities were the European Coal and Steel Community (1951), the European Economic Community (1957) and the the European Atomic Energy Community (1957). See: <Treaties Establishing the European Communities. https://europa.eu/european-union/sites/europaeu/files/docs/body/treaties_establishing_the_european_communities_single_european_act_en.pdf>

remains open to accession by "any State or international organization" (Art. 23.1, emphasis added). Thus, the IO has seven "Members" (and not Member-States), representing 34 countries, well over half the world's population, and most of its GDP as well. [18]

Other novel features of the Organization stem directly from its specialized nature, including the limited life of the project that resulted in a rather elaborate Article 24 on "Duration and Termination." This article of the ITER Agreement foresees an initial duration of the treaty (and the organization) of 35 years only. That the constitutive instrument foresees the organization's dissolution is still considered rather rare, [19]and has been mostly practiced by the so-called "commodity organizations." [20]

The temporary mindset has no doubt had an effect on many other aspects of the Organization's identity and on the Members' involvement. This has left the Members to decide how to best organize their respective participation and to what entity to assign the ITER portfolio. The treaty only requires that a "domestic agency" (DA) be appointed to coordinate the Member's contribution. [21] Depending on the Members, this could be an entirely new dedicated institution (such as the European DA created by a decision of the Council of the European Union) or a project under a ministry of energy working through a network of pre-existing labs (such as in the case of the US ITER Project Office within the Department of Energy), or some combination of these approaches.

This range of choices is due to another feature of the Organization: most of its resources (and therefore most of the Members' contributions) are supplied "in-kind." This means that the Members are providing the components which will make the machine, or they are building parts of the power plant themselves. Tracking the design, quality, compatibility, delivery and assembly is not only a coordination effort, but also a unique financial exercise. The complexity of the project is such, and the price tag of the

[18] ITER Organization current Members are China, EURATOM, India, Japan, Republic of Korea, Russian Federation, United States of America. See "What is ITER?", Factsheet by the European Domestic Agency (Fusion for Energy). <https://fusionforenergy.europa.eu/downloads/mediacorner/factsheets/2_Fact_sheet_Iter_light.pdf> accessed on 28 April 2020

[19] H G Schermers and N M Blokker, *International Institutional Law* (Leiden Brill | Nijhoff 2018), §1629.

[20] *Supra*, §1631.

[21] Art. 8.4 of the ITER Agreement states that "Each Member shall provide its contributions to the ITER Organization through an appropriate legal entity, hereinafter 'the Domestic Agency' of that Member, except where otherwise agreed by the Council. (...)".

resources differs so much from one Member to another, that the Organization uses its own currency: the ITER (kilo) Unit of Account[22] (ITER (k)IUA) to allocate credits among the Members on the basis of "Procurement Arrangements" passed between the Organization and each Member for the procurement of the various components and systems.

In the area of the Organization's privileges and immunities some novel but not surprising trends can also be noted. For instance, one such trend is to clearly define what is and is not in the definition of "official activities."[23] Another one is the relatively recent clarification on the exclusion of traffic offenses from the protections enjoyed by staff. Together they point at what some might consider the expression of the States' preference towards a more restrictive interpretation of the scope of the privileges and immunities enjoyed by both the Organization and its staff. The relative youth of the ITER Organization provided an opportunity for its Members to "codify" such interpretations in the relevant status instruments in a trend generally affecting newer international organizations.

Source: https://www.iter.org

Perhaps the most notable deviation from standard all-encompassing immunity from local law is the fact that the ITER Organization is subject to the laws and regulations of the Host State in the fields of public and occupational health and safety, nuclear safety, radiation protection, licensing, nuclear substances, environmental protection and protection from acts of malevolence (Article 14). While significant, this deviation is not, in itself,

[22] "The cost estimates for the construction and operation phases of the ITER Project have been quantified using the IUA unit of currency (IUA is the ITER Unit of Account and one IUA was equal to USD 1,000 in January 1989). The conversion rate from IUA to Euro is agreed yearly by the Management Advisory Committee of the IO in May. (Source: ITER organization Financial Report, 2013, at p. 7). Converted to euros at 2010 conversion rates (1 IUA = 1,552.24 euros), amounts to EUR 7.3 billion (Source: K. Dulon, 'Money Talks', I(TER Newsline 162, 4 Feb 2011) https://www.iter.org/newsline/162/576 accessed 28 April 2020

[23] Art. 5 of the ITER Privileges and Immunities Agreement exempts only "goods and services *strictly* necessary for the exercise of the official activities of the ITER organization" (emphasis added) and Art. 7 specifies which activities count as "official activities". Articles 5 and 8 of the Headquarters Agreement concluded between the Organization and the Host State (France) mirrors this language.

novel. Other international organizations are subject to local laws for parts of their operations (such as many of the International Financial Institutions for certain financial operations), and it is only understandable that France, as the Host State, has preferred to bring this international nuclear operator under its relevant laws and regulations.

One can see here another novelty: at ITER its nuclear identity—arguably the heart of its purpose is to build the fusion reactor for its Members—is placed under French law. If it had not been articulated in the treaty itself, this would have been quite a departure from the typical way the privileges and immunities of international organizations are formally arranged, perceived or even debated. The reality is that local law applies to the ITER administration (construction, management and operating) as an aspect of the capacity-building and prudent host nation support to a nuclear enterprise. The actual experimental and scientific cooperation as well as the Organization itself are regulated entirely by the ITER Agreement. The legal regime arising from the Agreement controls the single most valuable commodity of the Organization : the map to all the ITER knowledge.

Information and Intellectual Property: a regime within the regime

The ITER Agreement is not alone in providing the strategic international framework for the organization's role and activities. It is accompanied by two Annexes that form an integral part of the treaty and which provide further detail on matters of Site Support (Annex II), and, of particular relevance to the present note and section, Information and Intellectual Property (IP) with Annex I being called the IIP Annex. The IIP Annex describes at great length the IP regime for the ITER Project. This regime exists both within and parallel to the "real world" IP law and regimes. By appreciating the reach of IP law, the IIP Annex creates a web of rights and obligations between the Members and the Organization, including access rights, to all the information and intellectual property which will both go into the making of the machine and will result from its operation.

This is of cardinal importance. The Members will supply most of the ITER machine by in-kind contributions. Their research entities and industries will design or manufacture the components. They will all incorporate their own expertise and know-how; they will also undoubtedly discover new things. Innovation will be both incorporated as "background" and "generated" in the execution of the cooperative ITER project. Shared access to this innovation has to be managed.

National and international intellectual property law applies in parallel to the regime organized by the IIP Annex; and the two may often overlap. On the one hand, the ITER Members wanted to organize a specific regime to regulate their pooling and sharing of the knowledge. On the other hand, the laboratories or companies involved in the making of the components exist and operate under IP law regimes that regulate their sometimes-pre-existing technologies and know-how, their corresponding protections and licenses. There are also other considerations such as the various national research policies and obligations on all matters IP when using public funds. There will also be the experimental results and data once the machine starts operations. Realizing the difficulty of finding a solution in IP law, the Members found common ground by establishing rights and obligations, for themselves and for the Organization, to ensure the appropriate knowledge of and access to these technologies and results.

Thus, the IIP Annex regulates not only the general dissemination of information or results of the cooperation activities, but also establishes a matrix of access rights, depending on the ownership of the IP, and depending on its status and future use. For instance, the Members have the faculty to leave ownership of works generated in the execution of the ITER Agreement to their industries, or to own such works entirely or even jointly. However, they must ensure free access for the IO and the other Members to these results when access is requested for publicly sponsored fusion research and development. Access shall be ensured, but conditions may apply, if the intended use is for commercial fusion purposes or for use in fields outside of fusion. The ITER Organization itself has comparable obligations in this respect, but it also has the obligation to own the IP it created in execution of the Agreement.

"Execution of the Agreement" is a key phrase when identifying works which are likely to fall under its provisions. On the one hand, it is clear that anything created before the entry into force of the ITER Agreement is to be considered as "background" IP. In addition, technologies generated after the entry into force of the ITER Agreement but outside of its scope are also considered as "background" IP. The ITER Organization and the Members execute the Agreement by placing the various services or supply contracts necessary for the procurement of the ITER components. It falls on them to ensure that the contract has properly reflected the IIP obligations of the treaty. Thus, if incorporated third party background IP is necessary for the operation of the ITER machine, its maintenance or repair, or simply for the use

of the results of the contract, access rights will have to be ensured. For background IP—just like for generated IP—access rights will depend on multiple factors. These will include the intended use of the IP, its original ownership, and any pre-existing conditions for its use. The whole system results in a matrix of access rights based on licenses, rights to sub-license and to further develop. At the request of the ITER Council, this matrix is kept in an IP database which includes other 'IP-useful' information such as existing licenses, and scientific publications.

Scientific organizations typically have rather advanced and elaborate intellectual property policies, and have put in place the procedures and tools to review, clear, protect or disseminate the results of their activities. But if sister scientific organizations such as CERN, the European Organization for Nuclear Research, or ESA, the European Space Agency, focus much of their IP policies on managing the output, the ITER Organization has a specific mandate to also map the past—all of it—even if it belongs to other entities; and for reasons which go beyond the mere use or protection against infringement. The goal is to provide the Members with the complete map of the know-how, technology and skills used in delivering the machine, not by disclosing them, but by cataloguing their existence, provenance and any conditions attached to them.

The IP Database joins other databases in an incredibly sophisticated system of managing the project resources and documentation. This system supports the requirements of configuration management, nuclear safety and licensing, all of which are of vital importance to the science of the machine, but also to its operation as a licensed international nuclear operator on French soil.

Conclusion

This note only scratches the surface of the most prominent areas of ITER's multifaceted existence as a project and as an intergovernmental organization. As noted, certain aspects of the organization's set-up and governance may be common with other international organizations, but what undoubtedly makes the ITER Organization unique is how innovation permeates virtually every aspect of its existence and operation. From the very core of its forward-looking scientific and experimental mission, to the premeditated detail of the management of its legacy, the ITER Organization is

displaying a remarkable resemblance to its parents—a strong lineage of international and scientific organizations—but it is a child of its own time. And perhaps here lies the single most innovative feature of the organization: it may very well be a harbinger of the return to fashion of a new generation of intergovernmental organizations: those with a single mission, a timeline for its accomplishment, and a finite life and set of resources. If so, these would be international organizations of exceptional agility and capacity to deliver, all the while enjoying similar benefits as much as the challenges of sovereign and consensus-based traditional international organizations.

February 2020, Photo: ITER Organization/EJF Riche
Source: https://www.iter.org

Rear Admiral Sinan Azmi Tosun, the Commander of the NATO's Counter Piracy Mission, Operation Ocean Shield (left), and his Chinese counterpart Rear Admiral LI Shihong meet at sea, in the Gulf of Aden, on the Turkish Frigate TCG Giresun.
Source: https://www.nato.int/cps/en/natolive/news_83585.htm?selectedLocale=en

Partnership, Not Pivot: NATO's Legal Answer to the China Question[1]

by Lauren Brown[2]

The idea of innovation often conjures images of new capabilities, wrested from the realm of science fiction by dedicated visionaries and impressive advances in technology. However, such an understanding ignores one of innovation's most powerful potential for organizations: a critical agility in strategy and operations. Such innovation, or reinvention, in product, purpose, or strategy, is a common practice in the private sector, allowing brands and businesses to adjust to their evolving realities. Too often such

[1] The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, ACO or ACT.

[2] Lauren Brown works in Washington, DC, as an Associate in the International Trade Group of Squire Patton Boggs, a full-service global law firm. In 2019 she was the first NATO Legal Extern from the University of Georgia School of Law's Dean Rusk International Law Center in partnership with NATO Allied Command Transformation.

flexibility in strategy is absent in the realm of international organizations, however. Whether hindered by bureaucracy or constrained by their own founding charter's limited scope, international organizations may be slow to adjust their global strategies. The North Atlantic Treaty Organization (NATO) is guilty of the same unhelpful adherence to the way things were. As a result, the Organization is falling behind in addressing the multipolar reality that has defined the geopolitical landscape since the early twenty-first century. This multipolar world features as primary influencers the United States, the Russian Federation, and the People's Republic of China. And it requires NATO to undertake innovation in its strategy; in particular, to broaden its partnership initiatives formally to include China. Accepting the premise that partnership is preferable to an adversarial or ill-defined relationship, the question becomes twofold: First, can an organization established to "promote stability and well-being in the North Atlantic area"[3] engage effectively, while operating within its own legal framework, with the issues posed by the evolving global reality? Second, what would be the most effective partnership model within this legal framework?

This essay addresses these questions, exploring both the written and practiced NATO legal framework, and proposing three possible approaches to NATO's relationship with China. The first section discusses the purpose of NATO as evinced through the historical context of its creation. This section traces the evolution of the purpose of NATO and the implications of this evolution for the scope of NATO operations and partnerships, as such activities and relationships are prescribed by the Organization's founding document, the North Atlantic Treaty. The second section examines the legal framework in which NATO undertakes partnerships. Examined are the different structural mechanisms through which NATO establishes, and maintains, regional and bilateral partnerships. The third section discusses five potential models for partnerships with China. Based on the NATO legal framework and NATO practice, the models include: maintaining the Alliance's existing relationship with China; inviting China to form a formal bilateral partnership as part of the Partners Across the Globe framework; forming an organizational partnership with the Shanghai Cooperation Organization (SCO); creating an East Asia Partnership Group; and pursuing a non-relationship. The essay's fourth section concludes that the text of the North Atlantic Treaty and NATO practice provide the flexible partnership legal

[3] North Atlantic Treaty Preamble, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

framework in which the strategic innovation of a formal partnership with China can occur. It further argues that regardless of the mechanism of partnership, a formal partnership with China is necessary for NATO to remain relevant in a changing global reality.

I. Historical Context

Before undertaking an analysis of the NATO partnership framework, it is helpful to briefly describe the historical geopolitical context in which NATO and its legal infrastructure arose, as well as the evolving reality in which they continue to operate today.

A. Cold War

NATO is often understood as the Western foil to the Soviet bloc, born as a military and political counterbalance to Soviet power. This characterization is partially correct; however, the Alliance's creation also served to facilitate continental peace by promoting European political integration and stifling potential returns to the nationalist militarism that had plagued, and, in two world wars ravaged, Europe.[4] The North Atlantic Treaty was signed on 4 April of 1949, the same year the Soviet Union would become an atomic power.[5] Soviet nuclear capabilities, along with the outbreak of the Korean War in 1950, instilled an urgency in the Alliance. Early NATO leaders, including General Dwight D. Eisenhower and Lord Hastings Lionel Ismay, implemented the consolidated military command structure that defines the Organization to this day.[6] With the formation of the Warsaw Pact in 1955 and the construction of the Berlin Wall in 1961, NATO did, indeed, serve as the primary organizational antithesis to the Soviet Union and its expansionist ambitions. The Organization would remain in such a posture until, and arguably beyond, the fall of the Soviet Union in 1991.[7]

B. Post-Soviet Union

The collapse of the Soviet Union ushered in a new global reality. Similarly, NATO's purpose and function had to evolve in the wake of the apparent erasure of its greatest existential threat. Although the collapse of

[4] *A Short History of NATO*, NORTH ATLANTIC TREATY ORGANIZATION, available at https://www.nato.int/cps/en/natohq/declassified_139339.htm.
[5] *Id.*
[6] *Id.*
[7] *Id.*

the Soviet Union and the Warsaw Pact could have marked the end of NATO, there was no real indication within the Organization or amongst its Members that the experiment was over.[8] The end of the Soviet Union did not mean the end of threats to North Atlantic interests, and the Alliance shifted its attention from a consolidated adversary to a broader range of threats. During the 1990s, NATO's objective was "to demonstrate that it could project to the East the type of stability and security which hitherto only NATO members in the West have been able to enjoy."[9] This evolution in purpose and policy saw NATO engage with the post-Cold War world through expanded partnerships and out-of-area operations, including involvement with the conflict in the Balkans and Afghanistan.[10]

It is this more global-oriented NATO that must consider the question of a formal relationship with China. In recent years, China has drastically expanded its international influence. Indeed, some observers have even been prompted to forecast China's replacement of the United States as the world's dominant power.[11] From its Belt and Road Initiative[12] to its investment in foreign economies to its development of information technologies and cyber capabilities,[13] China's global initiatives are ambitious but not without controversy.

In early 2019, in a move largely viewed to be in direct response to a significant increase in Chinese investment in European Union Member States, the European Parliament voted overwhelmingly to increase scrutiny of foreign investments.[14] Additionally, security concerns surrounding Huawei, a telecommunications firm long suspected of having close ties to the Chinese government, and its bids to build several countries' 5G networks have led the United States to declare there is "no safe level" of interaction with the

[8] Jamie Shea, *How did NATO Survive the Cold War? NATO's Transformation After the Cold War from 1989 to the Present*, NORTH ATLANTIC TREATY ORGANIZATION, Nov. 6, 2003, available at https://www.nato.int/cps/en/natohq/opinions_20526.htm?selectedLocale=en .
[9] *Id*.
[10] *Id*.
[11] G. John Ikenberry, *The Rise of China and the Future of the West*, FOREIGN AFFAIRS, Jan./Feb. 2008, available at https://www.foreignaffairs.com/articles/asia/2008-01-01/rise-china-and-future-west .
[12] Andreea Brinza, *Redefining the Belt and Road Initiative*, THE DIPLOMAT, Mar. 20, 2018, available at https://thediplomat.com/2018/03/redefining-the-belt-and-road-initiative/ .
[13] See Sarah Cook, *Tech Firms Are Boosting China's Cyber Power*, THE DIPLOMAT, Sept. 25, 2018, available at https://thediplomat.com/2018/09/tech-firms-are-boosting-chinas-cyber-power/ .
[14] *With Eyes on China, EU Lawmakers Back Investment Screening*, REUTERS, Feb. 14, 2019, available at https://www.reuters.com/article/us-eu-china-investment/with-eyes-on-china-eu-lawmakers-back-investment-screening-idUSKCN1Q31JU .

company and to warn of re-evaluations of intelligence sharing relationships with countries that do allow Huawei to implement their 5G networks. [15] The controversy also resulted in the sacking of a British Cabinet Minister after he allegedly leaked information indicating the United Kingdom intended to work with Huawei on its telecommunication infrastructure.[16]

Accordingly, NATO's broader strategy of maintaining peace and security through a more expansive approach to global engagement is incomplete without a mechanism for addressing China. Such an initiative, including a potential formal partnership with China, is made possible through the proven flexibility of NATO's legal framework.

II. NATO's Legal Framework

Although partnerships with nations outside the North Atlantic Area are a well-established NATO practice, it is important to understand the legal framework underlying these initiatives. This discussion briefly surveys the basic legal framework in which partnerships occur, including the foundation in the North Atlantic Treaty and the specific partnership programs run by the Alliance.

A. The North Atlantic Treaty

In any examination of an international organization's legal framework, it is useful to begin with the group's founding documents, which indicate not only the principles on which the organization was founded but also provide insight into the envisioned legal scope and operational footprint of the organization. Accordingly, this analysis of the NATO legal framework opens with a brief discussion of the articles of the North Atlantic Treaty relevant to this essay's proposal to expand partnerships to include China.

1. Article 4

Article 4 of the North Atlantic Treaty grants NATO significant flexibility in its structure and operations. The relatively brief text states: "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is

[15] *Huawei: US Official Warns 'No Safe Level' of Involvement with Tech Giant*, BBC NEWS, Apr. 29, 2019, available at https://www.bbc.com/news/uk-48098362 .

[16] Larry Elliott, *The Huawei Incident Points to a Deeper Lesson for Britain*, THE GUARDIAN, May 5, 2019, available at https://www.theguardian.com/technology/2019/may/05/the-huawei-incident-points-to-a-deeper-lesson-for-great-britain .

threatened."[17] Because all NATO decisions are made by consensus, the consultation described in Article 4 is a critical part of the Organization's decision-making process.[18]

Considering China's geopolitical role as one of the major powers within the existing global regime, its domestic policies often cited as contrary to Western democratic values, and its intricate economic interactions with NATO Allies, any decision to bring the nation into a formal partnership with the Alliance would likely come from Article 4 consultation. The breadth of the language of the Article likely would also address any concerns regarding NATO's strategic expansion beyond its prescribed geographic scope of the North Atlantic Area.[19] As global realities change, Article 4 provides the Organization the flexibility to evolve and remain relevant while operating within its established legal framework.

2. Article 12

Article 12 of the North Atlantic Treaty serves the same underlying flexibility as discussed with Article 4. The Article states:

> After the Treaty has been in force for ten years, or at any time thereafter, the Parties shall, if any of them so requests, consult together for the purpose of reviewing the Treaty, having regard for the factors then affecting peace and security in the North Atlantic area, including the development of universal as well as regional arrangements under the Charter of the United Nations for the maintenance of international peace and security.[20]

This language indicates the importance of consultation amongst the Member States regarding, as stated in the article itself, "the factors then affecting peace and security in the North Atlantic area."[21] Indeed, at this point in time, well after the ten-year trigger point for Article 12, the only apparent limitation on the development of "universal" or "regional" arrangements[22] by the Alliance is that such efforts must take place in accordance with the Charter of the United Nations and be "for the

[17] North Atlantic Treaty art. 4, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
[18] *The Consultation Process and Article 4*, NORTH ATLANTIC TREATY ORGANIZATION, Mar. 17, 2016, available at https://www.nato.int/cps/en/natolive/topics_49187.htm .
[19] North Atlantic Treaty art. 12, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
[20] *Id*.
[21] *Id*.
[22] *Id*.

maintenance of international peace and security."[23]

As with Article 4, China's complex and extensive interactions with institutions and states in the "North Atlantic area" – even within that narrowest definition of that problematic term[24] – likely allows consultations regarding Alliance policy and strategy in addressing China and its global influence. The language of Article 12 is arguably broader than that of Article 4 as it appears to contemplate factors outside the North Atlantic Treaty's prescribed regional focus that have an impact within the North Atlantic Area. Accordingly, the drafters carefully crafted an Alliance in which the Member States could adapt the strategy and operations that are necessary to address an evolving geopolitical reality, including a potential formal partnership with China.

Source: https://natolibguides.info/partnerships

B. Partnership Models

Having established the articles in the North Atlantic Treaty that allow for formal partnerships with states outside the Alliance, it is important to understand the way in which current formal NATO partnerships programs function. NATO cooperates with more than forty countries through a combination of regional and bilateral partnerships.[25] The majority of these partnerships operate through a regional framework; however, as the international geopolitical landscape continues to shift and evolve, the Alliance does engage in formal and, at times, more informal bilateral partnerships. It is necessary to briefly discuss these partnership frameworks to

[23] *Id*.
[24] *See The North Atlantic Treaty Organization (NATO) In Transition*, ASSOCIATION OF THE UNITED STATES ARMY: AUSA BACKGROUND BRIEF, No. 60, Jan. 1994.
[25] *Partners*, NORTH ATLANTIC TREATY ORGANIZATION, Nov. 11, 2015, available at https://www.nato.int/cps/en/natolive/51288.htm.

better understand how China best could be brought into a formal partnership with the Alliance.

1. Partnership for Peace Programme

Begun in 1994, the Partnership for Peace Programme (PfP) works to develop bilateral relations between PfP participants and NATO. The partnership framework allows the individual relationships to consider issues and cooperation based on priorities unique to the particular bilateral reality.[26] Twenty-one countries belong to the PfP Programme, including Armenia, Austria, Azerbaijan, Belarus, Bosnia and Herzegovina, Finland, Georgia, Ireland, Kazakhstan, Kyrgyz Republic, Malta, Republic of Moldova, North Macedonia, Russia,[27] Serbia, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.[28] In 2011, the Alliance opened "all PfP activities and exercises" to all NATO partners, regardless of the specific partnership regime under which the partner nation cooperates with NATO.[29]

The Partnership for Peace: Framework Document, which established the PfP Programme, states that by entering into the partnership, the subscribing states and NATO Member States "recall that they are committed to the preservation of democratic societies, their freedom from coercion and intimidation, and the maintenance of the principles of international law."[30] This language appears to indicate the underlying concept of shared ideals amongst NATO Member States and PfP participants. Such democratic ideology could place limits on any initiatives aimed at expanding the PfP Programme to include China, given that the practices of this state appear not to have embraced democratic values – the regime has loosened, but remains Communist.[31] Accordingly, although PfP exercises have been opened to all partner nations, and although additional PfP membership seems possible upon invitation,[32] the legal framework under which the PfP

[26] *Partnership for Peace Programme*, NORTH ATLANTIC TREATY ORGANIZATION, Jun. 7, 2017, available at https://www.nato.int/cps/en/natohq/topics_50349.htm.
[27] Relations with Russia through the PfP Programme have been suspended since 2014 in response to Russian actions in Ukraine. *See Relations with Russia*, NORTH ATLANTIC TREATY ORGANIZATION, Feb. 4, 2019, available at https://www.nato.int/cps/ra/natohq/topics_50090.htm .
[28] *Partners*, *supra* note 23.
[29] *Partnership for Peace Programme*, *supra* note 24.
[30] North Atlantic Treaty Organization, Partnership for Peace: Framework Document, 1994.
[31] *See* Kenneth Rapoza, *Communist China is Now the Leader of the 'Free Trade' World*, FORBES, Jan. 24, 2017, available at https://www.forbes.com/sites/kenrapoza/2017/01/24/communist-china-is-now-the-leader-of-the-free-trade-world/#4b2ed4c121e0 .
[32] North Atlantic Treaty Organization, Agreement Among the States Parties to the North Atlantic Treaty and the

Programme was established, even if expanded, is unlikely to comfortably include China.

2. Euro-Atlantic Partnership Council

Established in 1997, the Euro-Atlantic Partnership Council (EAPC) operates as a "multilateral forum for dialogue and consultation on political and security-related issues among Allies and partner countries."[33] The EAPC consists of all NATO Member States, plus the 21 partner countries under the PfP Programme.[34] The Council meets monthly at the ambassador level and annually at the ministerial level.[35]

The EAPC facilitates cooperation on myriad matters through its Euro-Partnership Work Programme, including crisis-management and peace-support operations, arms control, international terrorism, and border security.[36] The Council is intended to provide the "overall political framework for NATO's cooperation with partner countries in the Euro-Atlantic area, and for the bilateral relationships developed between NATO and individual partner countries under the Partnership for Peace (PfP) programme."[37] Despite having members whose geography extends the EAPC well into Central Asia, the regional nature of the Council would likely make it a poor fit for any formal inclusion of China.

3. Mediterranean Dialogue

In 1994, the North Atlantic Council established the Mediterranean Dialogue.[38] Designed as a "forum for political consultations and practical cooperation,"[39] the Dialogue's structure features both bilateral and multilateral components.[40] Currently, it includes Algeria, Egypt, Israel, Jordan,

---

Other States Participating in the Partnership for Peace Regarding the Status of Their Forces, art. 5(3), Jun. 19, 1995.

[33] *Euro-Atlantic Partnership Council*, NORTH ATLANTIC TREATY ORGANIZATION, Jun. 9, 2017, available at https://www.nato.int/cps/en/natohq/topics_49276.htm .

[34] *Partners, supra* note 23. North Macedonia is set to become the 30th NATO Member State upon formal ratification.

[35] *Euro-Atlantic Partnership Council*, *supra* note 31.

[36] *Id.*

[37] *Id.*

[38] *NATO Mediterranean Dialogue*, NORTH ATLANTIC TREATY ORGANIZATION, Feb. 13, 2015, available at https://www.nato.int/cps/en/natohq/topics_60021.htm .

[39] *Questions & Answers: NATO's Mediterranean Dialogue & Istanbul Cooperation Initiative*, NORTH ATLANTIC TREATY ORGANIZATION, Feb. 9, 2012, available at https://www.nato.int/cps/en/natohq/topics_59419.htm .

[40] *Id.*

Mauritania, Morocco, and Tunisia;[41] however, it is formally open, as are most of NATO's regional partnership frameworks, to countries in the region or "directly involved" in regionally related processes.[42] Similar to the EAPC, despite some geographic flexibility in the framework, the regional focus of the Mediterranean Dialogue likely makes it a less desirable option for Chinese partnership.

4. Istanbul Cooperation Initiative

Established in 2004 at the NATO Summit in Istanbul, the Istanbul Cooperation Initiative (ICI) seeks to "contribute to long-term global and regional security by offering countries of the broader Middle East region practical bilateral security cooperation with NATO."[43] The ICI is composed of four countries, including Bahrain, Kuwait, Qatar, and United Arab Emirates, with both Saudi Arabia and Oman having expressed interest in joining.[44] Membership in the Initiative is officially "open to all interested countries of the broader Middle East region who subscribe to its aims and content, including the fight against terrorism and the proliferation of weapons of mass destruction."[45] However, the North Atlantic Council evaluates applicants on a case-by-case basis, emphasizing the applicant nation's indicated interest in cooperation with NATO, particularly regarding fighting terrorism and the proliferation of weapons of mass destruction.[46]

Although China has extensive interests in the Middle East,[47] the ICI's underlying purpose does not appear to best address shared points of interest between NATO and China.

5. Partners Across the Globe

Not all NATO partnerships operate within a regional framework. To address a complex, globalized world, the Alliance cooperates bilaterally with individual states designated as Partners Across the Globe.[48] These countries

[41] *Partners, supra* note 16.
[42] *Questions & Answers, supra* note 37.
[43] *Istanbul Cooperation Initiative (ICI),* NORTH ATLANTIC TREATY ORGANIZATION, Nov. 18, 2011, available at https://www.nato.int/cps/en/natohq/topics_58787.htm .
[44] *Id*.
[45] *Id*.
[46] *Id*. and *Questions & Answers, supra* note 37.
[47] *See* Nicholas Lyall, *China's Rise in the Middle East: Beyond Economics*, THE DIPLOMAT, Feb. 25, 2019, available at https://thediplomat.com/2019/02/chinas-rise-in-the-middle-east-beyond-economics/ .
[48] *Relations with Partners Across the Globe*, NORTH ATLANTIC TREATY ORGANIZATION, May 19, 2017, available at https://www.nato.int/cps/en/natohq/topics_49188.htm .

include Afghanistan, Australia, Colombia, Iraq, Japan, the Republic of Korea, Mongolia, New Zealand, and Pakistan.[49] An emphasis on the importance of cooperation with nations around the world underlies the Partners Across the Globe effort.[50] The 2010 Strategic Concept reiterated this idea, and further pushed NATO to revise its partnership policy as a means to engage better with global partners.[51] Global partners are able to participate in all NATO activities and operations open to partner states, and they can tailor their relationship with NATO through Individual Partnership Action Plans.[52]

The two primary strengths of this model are the lack of geographic specificity and the flexibility to tailor the terms of the relationship. The framework allows such flexibility while also maintaining the formality of an actual bilateral commitment. Such a structure makes the Partners Across the Globe initiative among the more relevant existing frameworks for a potential formal Chinese partnership.

6. Individual Partnership Action Plans

Individual Partnership Action Plans (IPAPs) work "to bring together all the various cooperation mechanisms through which a partner country interacts with the Alliance, sharpening the focus of activities to better support their domestic reform efforts."[53] The only real eligibility requirement to participate in an IPAP is that the non-Member country in question has "the political will and ability to deepen their relationship with NATO."[54] The IPAP establishes objectives and priorities of the partnership, allowing NATO to provide more focused advice regarding "defence and security-related domestic reform and, when appropriate, on larger policy and institutional reform."[55]

Although a helpful tool in establishing a constructive partnership, the dynamics involved in practice– namely, the Alliance's provision of advice and resources – do not seem to be relevant to China's domestic military, political, and economic realities.

---

[49] *Id*.
[50] *Id*.
[51] *Id*.
[52] *Id*.
[53] *Individual Partnership Action Plans*, NORTH ATLANTIC TREATY ORGANIZATION, Jun. 9, 2017, available at https://www.nato.int/cps/en/natohq/topics_49290.htm.
[54] *Id*.
[55] *Id*.

7. Other Partnership Tools

In addition to the previously discussed partnership frameworks, the 2010 Strategic Concept emphasized the importance of global engagement and partnership with nations and organizations, such as the African Union or European Union, across the globe.[56] Accordingly, NATO employs separate "policies, programs, action plans and other arrangements" as "partnership tools" in the Alliance's renewed effort to improve its partnership outreach.[57] These initiatives focus primarily on issues of interoperability and capacity building, and on support for reforms in domestic defense and security sectors.[58] Additionally, some partnership tools provide for more in-depth bilateral cooperation in more limited areas of interest.[59] Complementary to the formal bilateral and regional programs, moreover, NATO informally cooperates with other non-Member States on issues of shared concern.[60] Such an arrangement currently defines NATO's relationship with China.[61]

III. A China Partnership

Having established the NATO legal and partnership framework under which any formal partnership with China would be implemented, the discussion now turns to the most effective way in which the Alliance could undertake a formalized partnership with China based on existing frameworks and the global reality. These ways include maintaining the existing relationship, working with China under the Partners Across the Globe initiative, forming an organizational partnership with the Shanghai Cooperation Organization, creating the East Asia Partnership Group, or pursuing a non-relationship.

A. Maintain Existing Relationship

The first option is to maintain the status quo. Identifying the exact nature of the relationship between NATO and China could prove challenging,

[56] North Atlantic Treaty Organization, Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon, 2010.
[57] *Partnership Tools*, NORTH ATLANTIC TREATY ORGANIZATION, June. 24, 2016, available at https://www.nato.int/cps/en/natohq/topics_80925.htm .
[58] *Id*.
[59] *Id*.
[60] *Relations with Partners Across the Globe, supra* note 46.
[61] *See* Erik Brattberg, *Time for NATO to Talk About China,* CARNEGIE EUROPE, Mar. 26, 2019, available at https://carnegieeurope.eu/strategiceurope/78684 .

however. Since 2010, with the exception of a three-year hiatus between 2015 and 2018, NATO and China have engaged in an annual dialogue.[62] The talks between NATO and Chinese military staffs underscore NATO's recognition that "the security situation in the Asia Pacific region cannot be separated from that of the Euro-Atlantic and NATO has an interest in understanding how these linkages work."[63] Aside from ticking proverbial boxes of global engagement, however, it is unclear exactly what practical fruit these dialogues have borne over the years. The staff talks in 2018 delivered an "action list" of potential issues on which there could be "practical cooperation" between China and the Alliance, including improved speed of naval communications and Chinese participation in NATO School courses and NATO participation at China's Defense University.[64] The final action point of the 2018 meeting was an agreement to hold a follow-up meeting in 2019.[65] At this writing, no such meeting appears to have been scheduled.

Meanwhile, in April 2019 and against the backdrop of the previously discussed Huawei controversy and European Parliament vote, NATO ministers held the first formal talks regarding China as a threat.[66] The discussion ranged from concerns about China's activities in the Arctic Circle to fears of hacking of NATO Member States' communication networks, particularly if China is involved in the installation of new 5G networks.[67] Despite strong U.S. support for a shift in focus and characterization of China as a potential threat both to NATO and to its Members,[68] the Alliance remains divided on the point.[69]

Accordingly, it is unclear what exactly NATO considers its relationship with China to be at the moment. Maintaining this lack of clarity could have strategic advantages, however. If China is also unsure where it stands with NATO, this insecurity could encourage the country to engage in continued or even more in-depth discussions and exchanges, in an effort to better

[62] *NATO and China Resume Military Staff to Staff Talks*, NORTH ATLANTIC TREATY ORGANIZATION, June. 5, 2018, available at https://www.nato.int/cps/en/natohq/news_155840.htm .
[63] *Id*.
[64] *Id*.
[65] *Id*.
[66] James Marson, *China Threat Rises to NATO's Agenda*, THE WALL STREET JOURNAL, Apr. 2, 2019, available at https://www.wsj.com/articles/china-threat-rises-to-natos-agenda-11554225508 .
[67] *Id*. and Joel Gehrke, NATO Turns a Wary Eye Toward China, The Washington Examiner, Apr. 2, 2019, available at https://www.washingtonexaminer.com/policy/defense-national-security/nato-turns-a-wary-eye-toward-china.
[68] *Id*.
[69] Marson, *supra* note 64.

understand or define the relationship. The drawbacks to maintaining this status quo, though, largely outweigh any such potential positives. Prolonged uncertainty and lack of cohesive direction in an organization like NATO could lead to inconsistent and ineffective policies and operations. Without a more defined relationship with China, the Alliance is left with no real or practical means of addressing China's growing influence in the North Atlantic region and within Member States and partner nations.

05 Jun. 2018 - NATO and China resume military staff to staff talks
Source: https://www.nato.int/cps/en/natohq/news_155840.htm

B. Include China in Partners Across the Globe

An alternative to the status quo would be to formalize the relationship with China, bringing it into NATO under the Partners Across the Globe initiative. As previously discussed, although China is eligible for membership in other regional partnership frameworks under their respective texts and stated purposes, the regional focus of the established frameworks renders them poor fits for an effective integration of China into the broader NATO partnership scheme. In contrast, inviting China to join as a Partner Across the Globe would allow flexibility in the focus and priorities of the relationship, while ensuring the interactions occurred within a formal legal context.

The bilateral relationship could be formed along models similar to those forged with other states with which there exist both shared interests and

shared skepticism, like Pakistan or Russia.[70] Such a partnership framework would allow the Alliance and China to identify shared interests and to develop a formal process through which dialogue can be maintained even during times of potential tensions. The bilateral facet to such a relationship would ensure the issues are specific to those concerns shared by China and NATO, without requiring consideration of other influences or priorities.

C. Form an Organizational Partnership

Another potential framework is an organizational partnership. Such an option would include a multilateral structure in cooperation with the Shanghai Cooperation Organization (SCO). Formed in 2001, the SCO is a regional organization focused on economic and political cooperation amongst its members, which include Kazakhstan, China, Kyrgyz Republic, Russia, Tajikistan, and Uzbekistan.[71] The SCO is a logical potential partnership organization, as the majority of its members already have formal relationships with NATO.[72] Such a framework, similar to NATO's relationship with the African Union or the European Union, could be a useful mechanism for Alliance engagement with China. The more multilateral features of a partnership with SCO could reduce pressure points of contention between the Alliance and China and facilitate broader and more significant cooperation. Such cooperative communication could take place in a forum similar to the EAPC or Mediterranean Dialogue and enable a focus on issues of shared impact between the two regional interests.

The option to form the partnership, on bilateral, multilateral, or hybrid terms, allows both NATO and China to tailor the terms and focus of their partnership in a manner that could not only best serve each party's interest immediately but could also evolve so that changing global realities are better addressed.

D. Creation of East Asia Partnership Group

An alternative to working within an existing partnership framework is to create a new program designed from conception to address issues specific to NATO's relationship with China. China is rapidly consolidating hegemonic

[70] *Relations with Pakistan*, NORTH ATLANTIC TREATY ORGANIZATION, Apr. 4, 2019, available at https://www.nato.int/cps/en/natohq/topics_50071.htm and *Relations with Russia*, *supra* note 25.
[71] *About*, THE SHANGHAI COOPERATION ORGANISATION, Sept. 1, 2017, available at http://eng.sectsco.org/about_sco/.
[72] *Id*. and *Partners, supra* note 23.

power in the East Asian region.[73] Accordingly, NATO's engagement with China should include considerations of Chinese influence and actions within this region, including as they do or could impact nations with which NATO has an existing formal partnership. The option most efficient and consistent with NATO partnership doctrine and practice is to create an East Asia Partnership Group.

Similar to the doctrinal parameters of the other regional partnership groups, the East Asia Partnership Group would be open to any nation that is either located in the region or "directly involved" in regionally related processes.[74] Despite the fact the latter parameter appears to remain undefined, the constructive ambiguity of the threshold regional involvement could help bring in potential partner states, like Thailand or India, located on the periphery of the geographic area more traditionally understood as East Asia. As with the Mediterranean Dialogue and the Istanbul Cooperation Initiative, membership in another partnership framework would not exclude membership in the East Asia Partnership Group.[75] Accordingly, Japan, the Republic of Korea, and Mongolia, all now part of the Partners Across the Globe program,[76] could join the East Asia Partnership Group. Like the other regional groups and EAPC forum model, the partnership framework would provide a platform for dialogue and cooperation between the regional actors and NATO. The multilateral nature of this alternative also ensures that the other, smaller regional actors have a voice in matters impacting East Asian interests, helping to ensure neither Chinese nor NATO action in the region has unintended geopolitical consequences.

The creation of an East Asia Partnership Group would allow China to be secure in the representation of its own interests in a regional context within its formal relationship with NATO. The flexibility of a grouped partnership also helps to ensure that as emerging or evolving issues impact the region and its actors, the partnership framework can absorb and address such changes through open dialogue and cooperation. Such dialogue is critical in areas such as the South China Sea, where controversy and disagreement could potentially flare. NATO's established record with regional partnerships could help regional actors and the Alliance build stronger cooperative relationships

[73] Jennifer Lind, *Life in China's Asia: What Regional Hegemony Would Look Like*, FOREIGN AFFAIRS, Mar./Apr. 2018, available at https://www.foreignaffairs.com/articles/china/2018-02-13/life-chinas-asia .
[74] *Questions & Answers, supra* note 37.
[75] *Id.*
[76] *Partners, supra* note 23.

and navigate issues of geopolitical difficulty.

E. Non-Relationship

NATO's fourth option regarding China is to pursue a policy of a non-relationship with the country. Although seemingly against the foundational premise that partnership is preferred to an antagonistic or undefined relationship, this alternative does have some advantages. NATO is, according to some observers, at an existential crossroads.[77] Accordingly, there is a strong argument that the Alliance must define its own internal purpose, infrastructure, and missions before seeking to engage with new partners, particularly one requiring such varied and careful considerations as China.

NATO former Deputy Secretary General Rose Gottemoeller participates in the Xiangshan Forum, during a session on Artificial Intelligence and the Conduct of Warfare, in Beijing, China – 25 October 2018. © NATO
Source: https://www.nato.int/docu/review/articles/2019/04/05/nato-at-70-an-opportunity-to-recalibrate/index.html

Further, a non-relationship with China would not necessarily be characterized as adversarial or non-defined. A purposeful avoidance of meaningful engagement between the two entities could be as deliberate and practiced as any carefully crafted partnership. Additionally, the approach would not necessarily lead to instability or points of conflict. Allowing each entity to pursue its respective interests without any formal or

[77] *See* Emma Ashford, *NATO's Open Door Leads to an Identity Crisis*, WAR ON THE ROCKS, Jun. 23, 2016, available at https://warontherocks.com/2016/06/natos-open-door-leads-to-an-identity-crisis/ .

informal cooperative framework could enable each to achieve their own objectives. These objectives should not be assumed to be contradictory to one another.

The lack of a formal or informal relationship between NATO and China could create unnecessary and untenable risks to international peace and security, however. As previously discussed, through its network of economic and political investments, China has established significant relationships with NATO Member States and partner nations. This direct contact coupled with regional controversies, including the South China Sea, indicates the likelihood that NATO and Chinese interests will interact with increasing frequency. This reality further indicates the importance of a formally defined and structured relationship between NATO and China to ensure dialogue and cooperation triumph over antagonism and conflict.

Conclusion

The world in which NATO operates has been evolving since the Alliance's conception. To remain relevant, NATO's strategy and operations must also evolve. Partnerships are some of the most powerful and important tools of the Alliance's global engagement strategy, and the Organization should expand its existing partnership infrastructure to include China.

The text of the North Atlantic Treaty and NATO practice provide the flexible legal framework within which such strategic innovation could occur. Additionally, the Alliance has four primary means through which it could undertake a relationship with China. The first is to maintain the status quo of the existing relationship. This option would allow continuity with no additional investment but could leave the Alliance with no defined way in which to address China's growing influence amongst its Members and partners. An alternative option is to include China under the Partners Across the Globe program. This bilateral approach would provide flexibility in the structure and ensure individualized interests are represented. Another potential framework would be an organizational partnership with the SCO. Such a relationship would help to ensure NATO, Chinese, and regional interests are effectively managed. NATO's fourth option is to create an East Asia Partnership Group. This choice would provide a regional context to the Alliance's relationship with China, allowing the partnership to address not only bilateral issues specific to the country but also to enable NATO's structured participation in regional issues. Finally, the fifth option for the Alliance is to pursue a policy of non-relationship. Although this arrangement would not necessarily be

undefined or antagonistic, the certainty of the two entities' interaction on the global stage coupled with the uncertainty of the parameters of such interaction, absent any formal relationship, could allow instances of conflict.

Forging and maintaining international partnerships can be challenging. But such relationships are critical for the survivability of an organization. In facing the changing global reality in which China features as a prominent player, NATO must do more to address the country and its growing global influence through undertaking a formal partnership with China. Regardless of the specific approach it ultimately chooses, NATO's future relevance is contingent upon its ability to directly and formally engage China in a meaningful cooperative partnership.

***

Source: www.nato.int

Responsibility, Liability and Lethal Autonomous Weapon Systems[1]

By Theodora Vassilika Ogden[2]

With decreasing populations in Europe and the US, the size of NATO forces is set to shrink, in contrast to the projected growth in other regions.[3] In the future, autonomous systems may be a possible means to fill military capability gaps. In addition, these new systems could entail a human resource offset, introducing new challenges to commanders. According to leading researchers, autonomous technology has reached a point where the deployment of lethal autonomous weapons systems (LAWS) is achievable in the near future.[4] With this technology right around the corner, questions relating to responsibility and liability must be answered. Otherwise, nations

[1] The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, ACO or ACT. This article is part of a longer report titled *Responsibility, Liability and Lethal Autonomous Weapon Systems*.

[2] Theodora is a Fellow at the Human Security Centre and a graduate of the University of Manchester and Birkbeck, University of London, currently studying at Leiden University. She was previously a Legal Intern at NATO HQ SACT (2018-19). Before that, she worked at the Fundamental Rights Agency of the European Union.

[3] EDA (2018) The Impact of Demographic Change on Recruitment and Retention of Personnel in European Armed Forces, Opinions of Young Prospects and International Experts: Executive summary, April 2018.

[4] Geneva Academy of International Humanitarian Law and Human Rights (2017) Defending the Boundary – Constraints and Requirements on the Use of Autonomous Weapon Systems under International Humanitarian and Human Rights Law.

and their militaries run the risk of violating the Law of Armed Conflict (LOAC) and International Humanitarian Law (IHL). This article lays out the nuts and bolts of the issues that arise when we ask the question "who is responsible and liable if LAWS commit atrocities in the field?"

The US Department of Defense broadly defines an 'autonomous weapon system' as:

"*A weapon system that, once activated, can select and engage targets without further intervention by a human operator.*"[5]

Autonomy is a very complex notion, which is constantly evolving as technology develops in new directions; hence it is not possible to frame in a methodical definition. At this point, the idea of a working definition seems in keeping with the rapid development within the field of autonomy. In general, many observers are careful to provide a single definition, acknowledging that there are multiple interpretations, and varying degrees of autonomy. The Human-Machine command-and-control relationship, the sophistication of the machine's decision making, the type of decision or function being automated are all lines along which concepts of autonomy may vary.[6] Historically, the defining element of autonomous weapons was the ability to delegate authority to a machine.[7] A landmine fulfils this criteria, and Paul Scharre goes as far as to say:

"*The term 'autonomous robot', for example, might mean a house cleaning Roomba robot to one person and a science fiction* Terminator *to another!*"[8] The recently approved NATO definition of 'autonomy' offers a more updated, narrow interpretation:

"*A system's ability to function within parameters established by programming and without outside intervention in accordance with desired goals, based on acquired knowledge and an evolving situation awareness*."[9]

This definition indicates that there is a gradual move away from associating autonomy with landmines and Roombas, to an understanding of

[5] US Directive: Autonomy in Weapon Systems (DOD Directive 2012, November 21), Directive 3000.09.
[6] Scharre, Paul D. (2015) The Opportunity and Challenge of Autonomous Systems, Autonomous Systems: Issues for Defence Policymakers, The Hague: NATO Communications and Information Agency, p. 8.
[7] Schulman, Loren DeJonge & Simpson, Erin (2019) The Future of War: Autonomous Weapons, AI, and Cyberwarfare, 29 January 2019.
[8] Scharre, Paul D. (2015) Op. cit.
[9] NATO HQ SACT (2018) Current Taxonomy and legal considerations of the autonomy program, October 2018

autonomy that encompasses smart technology and deep learning.

There are considerable legal and ethical concerns being raised by the international community. Some are concerned that automated systems will lower the threshold of going to war.[10] Others argue that fully autonomous weapons would not be able to conform to the obligations on means and methods of warfare, as established in the Law of Armed Conflict.[11] The European Parliament passed a resolution on 12 September 2018, urging for an international ban on LAWS. The resolution was adopted with 82% of members voting in favour. Although it is non-binding, the resolution came hot on the heels of UN nations calling for a ban at the Convention on Certain Conventional Weapons (CCW) earlier in 2018, reflecting mounting pressure to ban the use of LAWS.

There are, however, indicators that LAWS are here to stay. China joined the United Nations CCW in April 2018. Despite expressing doubts as to whether national regulations are sufficient, and even going so far as to support an outright ban,[12] there are reports of multiple advanced autonomous systems programmes being developed and tested in China.[13] In addition, five states have explicitly rejected efforts to introduce new international law banning fully autonomous weapons: France, Israel, the United Kingdom, the United States, and Russia.[14] Instead, these proponents advocate for the application of LOAC to be recognised in the context of LAWS.[15]

The view held by proponents of LAWS is that armed forces that do not have fully autonomous systems may not be able to match an adversary who does.[16] Additionally, some advocates argue that systems tethered to a human controller (e.g. UAVs) are becoming more susceptible to cyber-attack and interference. Some experts find that tethered systems are perhaps better

[10] PAX (2014) 8 objections to killer robots.
[11] Human Rights Watch (2012) Losing Humanity: The Case against Killer Robots.
[12] Busby, Mattha & Cuthbertson, Anthony (2018) 'Killer Robots' Ban blocked by US and Russia and UN Meeting, the Independent, 3 September 2018.
[13] The Inquirer (2018) China recruits 'patriotic' teens to work on autonomous weapons.
[14] The states which have endorsed the call for a ban on LAWS include: Algeria, Argentina, Austria, Bolivia, Brazil, Chile, China, Colombia, Costa Rica, Cuba, Djibouti, Ecuador, Egypt, El Salvador, Ghana, Guatemala, Holy See, Iraq, Mexico, Morocco, Nicaragua, Pakistan, Panama, Peru, State of Palestine, Uganda, Venezuela, Zimbabwe.
[15] Davey, Tucker (2018) Lethal Autonomous Weapons: An Update from the United Nations, April 2018, Future of Life Institute.
[16] Klare, Michael (2019) Autonomous Weapons Systems and the Laws of War, March 2019, Arms Control Association.

replaced by autonomous ones.[17] Furthermore, with better calculating abilities, as well as faster data analysis and manoeuvring capabilities, some supporters believe that machines will be able to perform more ethically and effectively than human soldiers.[18] Indeed, systems will not possess human weaknesses, such as fatigue, stress and anger, which may influence judgement.

LAWS raise issues in IHL, most notably the principles of distinction and proportionality. Some commentators argue that although autonomous weapon systems could be used in indiscriminate and non-proportional ways, they do not inherently violate these principles by possessing autonomous capabilities.[19] The issues raised by IHL are important and extensively covered elsewhere, most notably, by Lt. Col. Alan Schuller.[20] He examines the interaction of AI and machine learning in LAWS with IHL, providing an in-depth assessment across the four principles of distinction, proportionality, military necessity and the prohibition against causing unnecessary suffering. This article complements such work by addressing some of the more practical legal aspects concerning responsibility and liability.

Furthermore, this article distinguishes between the 'macro' decisions (i.e. defining missions at the strategic and operational level) and 'micro' decisions (i.e. those made at the tactical level on the battlefield). It is important to make this distinction, as it is generally foreseen that automated decisions will be made at the micro level, and macro decisions over target parameters, geographical/spatial boundaries and temporal boundaries will continue to be made by humans in the near future.[21] It would be useful for this distinction to be made elsewhere, as otherwise statements such as "life and death decisions will be made by robots" are misleading.

In addition, the author assumes that systems will be readable, i.e. allowing the user to "read" an activity log after action, to understand what

[17] Thurner, Jeffrey S. (2010) No one at the controls: Legal Implications of fully autonomous targeting, JFQ Issue 67, 4th Quarter 2012.
[18] Prof. Ronald Arkin, cited in Carafano, J. (2014) Autonomous Military Technology: Opportunities and Challenges for Policy and Law, The Heritage Foundation, 6 August, 2014.
[19] Crootof, Rebecca (2015) The Varied Law of Autonomous Weapon Systems, Autonomous Systems: Issues for Defence Policymakers, The Hague: NATO Communications and Information Agency, p. 106.
[20] Schuller, Alan (2017) At the Crossroads of Control: the Intersection of Artificial Intelligence in Autonomous Weapons Sytems with International Humanitarian Law, Harvard National Security Journal Vol. 8.
[21] Homayounnejad, Maziar (2017) Ensuring Lethal Autonomous Weapon Systems Comply with International Humanitarian Law, A Dickson Poon Transnational Law Institute, King's College London Research Paper Series.

the system has done and why.[22] Indeed, it would be almost impossible for an unreadable system to pass a weapons legal review. Including the readability feature is essential to preserving accountability, reliability and liability. At the Defense Innovation Board (DIB) Roundtable on AI Ethics and Principles, one participant suggested that it would be more costly to build a system with the necessary degree of readability, potentially giving up some efficiencies in the system.[23] Aside from asking questions about cost, we should also establish the extent to which the inclusion of a readability feature would diminish the level of autonomy and efficiency.

This article is therefore limited by the assumption that future LAWS will be readable for the most part, predominantly overridable and capable of only making micro decisions. This may contrast with other literature reflecting how AI systems and LAWS are perceived in the civilian sector, particularly by NGOs, the public and popular media.

Bridging the "responsibility gap"

If LAWS are employed and their actions violate IHL, who is to be held responsible? Is it the state, the Joint Force Command, the manufacturer, or perhaps the person who conducted the weapons legal review? Some experts suggest that this so-called 'responsibility gap' proves that LAWS are unlawful.[24] Others maintain that a gap will never exist as there will always be a human involved in the macro decision to deploy LAWS, to whom responsibility could be attributed.[25] However, the latter assumption determines that decisions made by LAWS at the micro level fall under the responsibility of the Joint Force Commander, rather than the programmer or the weapons legal reviewer. The reality is far more complex.

Domestic policy can — and does — change, meaning that there are no guarantees for the future, even on issues such as human oversight and authority. On their own, national frameworks do not offer a sufficient response to LAWS, as they provide narrow interpretations and vary from state to state.[26] This article seeks to move away from such regulations, pursuing more

[22] Barniuk, Chris (2017) The 'creepy Facebook AI' story that captivated the media, BBC News, 1 August, 2017.
[23] Defense Innovation Board (DIB) (2019) Summary of Defense Innovation Board (DIB) Roundtable on AI Ethics and Principles, Harvard University, 22 January 2019.
[24] ICRC (2014) Expert Meeting on 'Autonomous weapon systems: technical, military, legal and humanitarian aspects, 26-28 March 2014, Geneva.
[25] ICRC (2014) Op. cit.
[26] Article 36 (2016) Article 36 reviews and addressing Lethal Autonomous Weapons Systems, Briefing paper for delegates at the Convention on Certain Conventional Weapons (CCW), 11-15 April 2016, Geneva.

consistent sources of law. These are the three main legal frameworks that may apply to LAWS:

1. International law, which emphasises the law of state responsibility;
2. Individual criminal responsibility;
3. Manufacturer's liability (for example, the obligation to mitigate the consequences of negligence or breach of contract).[27]

International Law

Until there are precedents concerning the issue of autonomy, the legal implications of deploying weapons systems remain unclear. Although LAWS are being developed and used, there are no treaties specifically addressing such systems. Article 36 of 1977 Additional Protocol 1 to the 1949 Geneva Conventions concerns the "study, development, acquisition or adoption of a new weapon, means or method of warfare".[28] In theory, this obligation applies to every state party to the Protocol, regardless of whether it develops and manufactures weapons or purchases them.[29] In practice, out of the 174 states who ratified Additional Protocol 1, only between 15 and 20 states conduct their own legal reviews.[30] Many states who purchase weapons from other nations simply rely on reviews conducted by the selling state.

There are three limitations to Article 36. First, states are not obligated to make their legal reviews available to others, as this would give up their military advantage. However, in accordance with Article 84 of the Protocol, they are required to share their reviewing procedures with other states parties to Additional Protocol 1. Although it may be determined that a state has stringent legal review criteria, it is another matter entirely whether they actually employ them. Second, there are no concrete international standards for weapon reviews. There are indeed standards within the LOAC, with which weapons must comply, but there is little guidance for states conducting reviews. Instead, it is up to individual states how they wish to conduct their legal reviews. Third, there are no mechanisms to ensure international oversight or compliance with Article 36.[31] This makes it difficult to hold states to account and determine liability. As a consequence, this presents a significant

[27] ICRC (2014) Op. cit.
[28] Protocols Additional to the 1949 Geneva Conventions.
[29] Daoust, I. et al. (2002) New wars, new weapons? The obligation of States to assess the legality of means and methods of warfare, IRRC 84 (846), June 2002.
[30] ICRC (2010) Legal review of new weapons: Scope of the obligation and best practices.
[31] Article 36 (2016) Op. cit.

interoperability challenge for NATO to navigate. Without a solid framework in place, legal practitioners are unprepared for the next generation of weapons systems.

The ICRC finds that as well as for new weapons, reviews must be carried out for existing weapons that have been modified in a way that alters their function, or a weapon that has already passed the legal review but is subsequently modified.[32] Farrant and Ford provide the example of the Joint Direct Attack Munition (JDAM), a guidance package that is installed on unguided bombs, thereby converting them into satellite-guided "smart" munitions.[33] Standing alone, the JDAM is not a weapon, however, the unguided bomb that the JDAM is attached to is a weapon. Therefore, when the JDAM is installed on the bomb, this creates an entirely new weapon, which must undergo a weapon review.[34] The rules are clear in the event of hardware changes, however this is not necessarily the case for software changes. System updates and improvements to autonomous weapons may alter the initial function of the weapon. The degree of change to a system's software that would require a renewed legal review must be established.

The United Nations General Assembly adopted a draft resolution on the responsibility of states for internationally wrongful acts. In its Articles 1 and 2, the state is held accountable for an action or omission "attributable to the State under international law".[35] The state shall also be held responsible for the conduct of an individual or non-state entity, provided they are acting under the authority of the state "in the particular instance".[36] If a commander, acting under the authority of a state, deploys LAWS, this is an action for which the state could be held accountable.

However, should the weapons system make its own decisions in the field, could the state be held accountable for them? The CCW firmly places the responsibility of the actions of LAWS with states: "States must ensure accountability for lethal action by any weapon system used by the State's forces."[37] Conversely, other experts propose that machines with a sufficiently

[32] ICRC (2006) Op. cit., p. 10.
[33] Farrant, James & Ford, Christopher M. (2017) Autonomous Weapons and Weapon Reviews: The UK Second International Weapon Review Forum, International Law Studies 93, US Naval War College, p. 404
[34] Farrant, James & Ford, Christopher M. (2017) Op. cit.
[35] UN General Assembly (2002) Resolution adopted by the General Assembly, 56/83. Responsibility of States for internationally wrongful A/RES/56/83, 28 January 2002.
[36] UN General Assembly (2002) Op. cit. Art. 5.
[37] Convention on Certain Conventional Weapons (CCW), Meeting of Experts on Lethal Autonomous Weapons

high level of autonomy may become more similar to private actors than machines – at which point their actions may no longer be directly attributable to states.[38]

If a system makes a harmful decision on the tactical level, resulting in civilian casualties, which state is to be held responsible? Would the state that decides to deploy a system be held to account, but not the state in which the system was built and programmed? If the micro decisions – which LAWS are programmed to make – are being contested, the state in which the system was manufactured may share the responsibility. However, this becomes problematic if the state in which LAWS were manufactured are not party to Additional Protocol 1 of the Geneva Convention.

With the current lack of regulation in the field of LAWS, states which are not party to Additional Protocol 1 could produce weapons systems, export them and not suffer the consequences, should their LAWS commit atrocious acts on the battlefield. Indeed, Article 6 of the United Nations General Assembly draft resolution states:

"The conduct of an organ placed at the disposal of a State by another State shall be considered an act of the former State".[39]

This firmly places the responsibility with the state that uses the LAWS, rather than the state that developed them. While Article 6 may be useful in its application to non-autonomous weapons, this principle should not apply to systems with deep learning abilities. As well as potentially encouraging reckless behaviour by manufacturing states, the uncertainty surrounding the issue of liability hampers the development of artificial intelligence and the establishment of common standards.

As well as international human rights law, LAWS are set to be regulated by other international laws, such as the law of the sea, space law and aviation law, depending on the arena. At sea, the autonomous weapon system *Phalanx CIWS* has been in use by various navies since the 1980s. In addition to being affixed to ships, LAWS may be granted warship status, such as the *Sea Hunter*, a 132-foot long prototype Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV), developed by Defense

Systems (LAWS),11-15 April 2016, Geneva.
[38] Scharre, Paul D. (2015) Op. cit., p. 116.
[39] UN General Assembly (2002) Op. cit.

Advanced Research Projects Agency (DARPA).[40] The same international rules that apply to manned vessels will apply to autonomous vessels. According to the UN Charter, a warship's flag state bears "international responsibility for any loss or damage to the coastal state resulting from the non-compliance".[41] Similarly, airborne weapon systems will probably be bound by international aviation laws. An emerging challenge to be faced is how future laws regulating autonomous systems can be combined with existing international laws.

Source: https://www.innovationhub-act.org

Individual & Manufacturers Liability

Existing criminal and civil law leave significant room for interpretation. Prolific technology author John Kingston asks the following: could a malfunctioning programme claim a defence similar to the human defence of insanity? If it is affected by malware, could it claim defences similar to coercion or intoxication? Indeed, under criminal law, who is punishable for an offence for which an AI system was directly liable?[42] A *mens rea* ("guilty mind") is required to establish criminal liability, but it remains unclear how an autonomous system could fulfil this criterion.

Kingston speculates whether AI programs could qualify as innocent agents, such as animals, children, or persons with intellectual disabilities. Conversely, philosopher John Sullins, an expert in computer ethics, suggests that moral agency does not necessarily come with full technical autonomy, providing the examples of bacteria and viruses. Although such organisms are indeed autonomous, they are not considered moral agents.[43] He goes on to argue that an autonomous system would need to perceive and understand

[40] Cavas, Christopher P. (2016) Unmanned Sub-Hunter to Begin Test Program, Defense News 7 April 2016.
[41] UN (1982) United Nations Convention on the Law of the Sea, Territorial Sea and Contiguous Zone, Article 31.
[42] Kingston, J. K. C. (2018) Artificial Intelligence and Legal Liability.
[43] Sullins, J. (2006) When is a robot a moral agent? International review of information ethics 10 (6), pp. 23-30.

its role and responsibility to be considered a moral agent.[44] Instead, the responsibility may lie with individuals in the operating or reviewing process.

The responsibility of the individual can also be linked to international criminal law. In accordance with Article 25 of the Rome Statute of the International Criminal Court, an individual who commits one of the international crimes (genocide, crimes against humanity, war crimes, and the crime of aggression) will be held "individually responsible and liable for punishment".[45] However, as a participant at the ICRC expert meeting pointed out, it would be a considerable challenge to identify a specific individual in the complex development and manufacturing chain, and even more difficult to prove it.[46]

To better understand the issue of liability in the context of criminal law, we must look to the civilian sector, particularly with the emergence of self-driving cars. Under US law, users or programmers might be held legally liable if they knew that a criminal offence was a *natural and probable consequence* of using a system. Article 28 of the Rome Statute of the International Criminal Court states that a military commander "shall be criminally responsible for crimes within the jurisdiction of the Court committed by forces under his or her effective command and control".[47] However, it remains unclear whether the joint Force Command ought to be held responsible for the actions of autonomous (and sometimes unpredictable) weapons.

In the US, in the event of a car-crash involving automated cars, laws concerning 'faulty design' are likely to apply. Kingston observes: "settlements for product design cases are typically almost ten times higher than for cases involving human negligence, not including the extra costs associated with product recalls to fix the issue."[48] Vehicle manufacturers Volvo, Google, and Mercedes have already accepted full liability if their autonomous vehicles cause a collision. However, smaller, independent companies may not be able to accept the financial burden of full liability. This may manifest in a reluctance to develop autonomous technology in the civilian sector, which in turn affects developments in the military sector. Placing full responsibility with the developer could hold back the advance of autonomous technology.

[44] Sullins, J. (2006) Op. cit.
[45] International Criminal Court (2002) Rome Statute of the International Criminal Court, p. 17.
[46] ICRC (2014) Op. cit.
[47] International Criminal Court (2002)Op. cit., p. 19
[48] Kingston, J. K. C. (2018) Op. cit.

The British Ministry for Transport published proposals for self-driving cars, claiming that "existing common law on negligence should largely be able to adapt to this new technology". The proposals include three main points:

1. Recording data will be required to determine whether the driver or the vehicle was responsible for any collision.
2. Failure to maintain the automated vehicle technology, inappropriate use, and circumventing automated vehicle technology shall be taken into account when determining liability.
3. If an accident occurred as a result of an automated vehicle being hacked, it should be treated in the same way as an accident caused by a stolen vehicle.[49]

Some aspects may be transferrable to the military context. First, recording data may prevent incidents from occurring in the first place; monitoring the systems will enable the commander or operator to detect and shut down 'rogue' LAWS. In the aftermath of an incident, the data collected may be used to determine liability. It is generally assumed that LAWS must have this readable element to comply with the weapons legal review. Second, properly maintaining the system must be a priority, and relevant rules and procedures should be put in place. Third, in the civilian context, hacking would mean that the insurance company would have to compensate a collision victim, which could include the 'not at fault driver'. In the LAWS context, this scenario would be more complicated, although presumably the state or non-state actor who did the hacking would be held responsible.

Moving forward: recommendations

Human control

John Boyd developed the "observe, orient, decide, act" (OODA) loop, a popular concept in military strategy.[50] In combat, a soldier must complete their own decision loop as quickly as possible, while at the same time getting "inside", or interrupting, the opponent's OODA loop. Existing technologies generally keep humans "in the loop". However, future "on-the-loop" systems will carry out most of the mission without human operators, although a human can intervene or abort the mission.

[49] Centre for Connected and Autonomous Vehicles (2016) Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies, UK Department for Transport.
[50] John R. Boyd, *Destruction and Creation*, 3 September 1976, U.S. Army Command and General Staff College.

UK policy insists that the "operation of weapon systems will always be under human control",[51] committing to not use highly automated systems.[52] However, some observers raise the issue of semantics; the UK currently defines autonomous weapons systems as being "capable of understanding higher-level intent and direction". [53] According to the British non-profit organisation Article 36, this "places them in the realm of science fiction, far beyond the parameters within which most states are debating these systems".[54] Campaigners fear that this definition could render statements such as "the UK will not develop or acquire autonomous weapons" misleading.[55] It is essential that a standardised definition of 'autonomy' is developed at the international level, otherwise the legal waters will remain murky.

US guidelines state 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."[56] This policy does not go on to define an appropriate level of human judgement. Commentators point out that such an assessment may be different for different systems, "depending on the operating environment and the type of force used".[57] The US Department of Defense Directive 3000.09 also uses the term 'meaningful human control' (MHC). This principle is used at all levels and on all sides of the LAWS debate. An open letter signed by 1000 tech experts including Stephen Hawking, Steve Wozniak and Elon Musk famously called for a ban on "offensive autonomous weapons beyond meaningful human control".[58]

The term MHC was originally coined by the organisation Article 36, which defines it as permitting humans to determine "when, where and how weapons are used; what or whom they are used against; and the effects of their use."[59] Article 36's concept of MHC calls for meaningful human control

[51] Ministry of Defence (2013) Written Evidence from the Ministry of Defence submitted to the House of Commons Defence Committee inquiry 'Remote Control: Remotely Piloted Air Systems - current and future UK use', September 2013, p. 3.
[52] ICRC (2014) Op. cit.
[53] Article 36 (2018) Lords AI committee: UK definitions of autonomous weapons hinder international agreement, 17 April 2018.
[54] *Ibid.*
[55] Article 36 (2018) Shifting definitions? The UK and 'autonomous weapons systems', 23 July 2018.
[56] US Directive: Autonomy in Weapon Systems (DOD Directive 2012, November 21), Directive 3000.09.
[57] ICRC (2014) Op. cit.
[58] Future of Life Institute (2015). Autonomous Weapons: An Open Letter from AI & Robotics Researchers, Future of Life Institute.
[59] Article 36 (2015) Killing by Machine: Key issues for understanding Meaningful Human Control.

over individual attacks. However, the phrase is frequently used without this modifier, leading to various interpretations, such as MHC over weapon systems as a whole.[60] Some view meaningful human control to be a general principle for the design and use of weapon systems, to ensure that their use can comply with the laws of war.[61] Anti-LAWS campaigners point to the challenges or inability of establishing MHC as a reason to ban autonomous weapon systems.[62] The concept of MHC needs to be discussed and defined at the international level. In particular, what is meant by 'meaningful', (loosely interpreted to mean the quality of control)[63] and 'control' could be usefully discussed.

Legal reviews

Article 36 of Additional Protocol 1 to the Geneva Convention calls for 'new' weapons or means or methods of warfare to be assessed against all relevant rules of international law. It remains unclear what constitutes 'new' in Article 36.[64] The Tallinn Manual maintains that any 'significant changes' to an existing system necessitate a new legal review.[65] However, this becomes problematic in the context of autonomous technology, where systems continuously learn and adapt, and the outcomes are not entirely predictable. In conducting the initial review of the system, it is important for reviewers to understand what the system will be exposed to, and how this could affect its learning.[66]

In general, the principles of Article 36 could be expanded upon to ensure testing and reviewing LAWS at every stage of development, from initiating research, to the regular maintenance of deployable systems. The concept of Verification and Validation (V&V) is well-established in weapons design but needs to be integrated into the legal review process, along with greater transparency concerning the use of LAWS. At the ICRC Expert Meeting, participants emphasised the need to develop more precise

[60] UNIDIR (2014) The Weaponization of Increasingly Autonomous Technologies1 : Considering how Meaningful Human Control might move the discussion forward, p. 2.
[61] Horowitz, Michael C. & Scharre, Paul (2015) Meaningful Human Control in Weapon Systems: A Primer, Working Paper, Center for a new American Security, p. 7.
[62] UNIDIR (2014) Op. cit., p. 2.
[63] UNIDIR (2014) Op. cit., p. 3.
[64] Farrant, James & Ford, Christopher M. (2017) Autonomous Weapons and Weapon Reviews: The UK Second International Weapon Review Forum, International Law Studies 93, US Naval War College.
[65] Talinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, p. 129.
[66] Farrant, James & Ford, Christopher M. (2017) Op. cit., p. 407.

regulations for testing and reviewing LAWS.[67] At present, states which do not develop or manufacture weapons themselves – instead purchasing them from other nations – may rely on reviews conducted by the selling state.[68] This throws up a host of legal issues, as under current international law, states are held responsible for the weapons they deploy.

The DOD Directive 3000.09 requires two separate legal reviews for LAWS. The first review is conducted before a weapon system enters formal development. In this stage, the system must accommodate "appropriate levels of human judgment over the use of force".[69] The second review takes place at a later stage of development, ensuring that requirements have been implemented. In this stage, the review ensures that "adequate training, TTPs [tactics, techniques, and procedures], and doctrine are available, periodically reviewed, and used by system operators and commanders to understand the functioning, capabilities, and limitations of the system's autonomy in realistic operational conditions."[70] Although the United States is not yet party to Additional Protocol 1, there has been a lot of investment into the legal implications of LAWS, meaning that there are some elements of US defence policy that could be adopted by the international community.

To Autonomy and beyond: what the future holds

Before autonomous systems become widely used on battlefields, in all likelihood they will dominate everyday life. Siciliano and Khatib claim that "tomorrow, robots will be as pervasive and personal as today's personal computers."[71] From self-driving cars, to robots becoming common in the medical and judicial fields, it is likely that the public will become used to living with autonomous systems.

On battlefields, LAWS are predicted to move into roles relating to logistics, intelligence, surveillance and reconnaissance. In addition, the US Army pamphlet predicts that autonomous systems will be used to recover wounded soldiers from high-risk areas, with minimal exposure. Future soldiers will use unmanned vehicles, robotics, and advanced standoff equipment to

[67] Convention on Certain Conventional Weapons (CCW),Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS),11-15 April 2016, Geneva; Views of the International Committee of the Red Cross (ICRC) on autonomous weapon systems, 11 April 2016.
[68] Daoust, I. et al. (2002) Op. cit. p. 361.
[69] Directive 3000.09 Op. cit.
[70] Directive 3000.09 Op. cit.
[71] Siciliano B., Khatib O. (2008) Springer handbook of robotics, Berlin: Springer, p. 1.

allow for immediate evacuation, transfer and en route care under difficult conditions.[72]

The development of autonomous systems will likely increase human activity in space. Devices will be able to move freely in an oxygen-free environment. With the feature of autonomy, untethered systems will not be limited by factors such as visibility, communication distance and delay.[73] It is therefore likely that the development of autonomous systems will open up Space as a battleground for future warfare. Indeed, NATO has moved forward with the declaration of Space as an operational domain. States are dependent on the security of their satellites, which are also essential for communication, navigation, and powering entire economies and energy systems. States which do not invest in autonomous technology for space defence systems will be vulnerable to crippling attacks on their entire economy and infrastructure.

At this time, it is not possible to provide concrete answers to the question of who is liable if LAWS go rogue. However, this is a question that will have to be answered. A solid international legal framework for autonomous technologies will enable developments in academia and encourage innovation and investment in systems, as clear international standards and rules are set. Once the issue of liability and responsibility begins to be resolved, the field of robotics and autonomous systems will experience a surge, as smaller technology developers become more confident. Most importantly, the development of common standards and regulations will help avoid violations of International Humanitarian Law and the Law of Armed Conflict. It is important that this legal framework is developed in anticipation of this emerging technology. Considering the potential cost to human life, it is vital that this regulation is not shaped in a reactive manner, such as in the case of the policymaking on landmines, which only occurred long after atrocities were committed.

***

[72] Department of the Army (2008) Force Operating Capabilities Pamphlet (Pam) 525-66, Virginia.
[73] Kowalczuk, Zdzisław & Czubenko, Michał (2011) Intelligent Decision–Making System for Autonomous Robots, Int. J. Appl. Math. Comput. Sci. 21 (4), pp. 671–684.

Source: www.nato.int

Autonomous Weapon Systems: A Pragmatic Approach to an Emerging Capability[1]

By Major Gregg F. Curley[2]

I. Introduction

Autonomous weapon systems (AWS) are already a reality for NATO nations. Significant advances in computers, artificial intelligence, communications, and robotics will only make them more prolific. As a result, humankind is at the precipice of a paradigm shift in the very character of warfare. Many stakeholders have identified significant concerns and proposed various ways to regulate AWS, a challenge that will be a

[1] The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO or ACT.

[2] Major Gregg Curley, USMC, is currently serving as the Complex Trial Counsel (prosecutor) for Marine Corps Base Hawaii. Previous assignments include Civil Affairs Team Leader (Afghanistan), Aide-de-Camp, Defense Counsel, and Special Assistant US Attorney. Major Curley holds a Masters of Military Studies (USMC Command and Staff College); Masters in Military Operational Art and Science (Air Command and Staff College); LL.M. (The Judge Advocate General's School), J.D. (Roger Williams School of Law); and a B.S. and MBA (Sacred Heart University).

"...crossing of a moral Rubicon."[3] The scholarly writing on the topic adequately identifies the legal, ethical, and moral issues inherent in the employment of AWS and even provides some narrowly-scoped solutions.[4] This paper will provide the background necessary for international readers to address AWS, discuss the anticipated benefits and perceived drawbacks to the technology, and explain why an international ban of AWS is unlikely. Next, this paper will address the legal, ethical, and moral framework to which AWS must adhere and then synthesize the disparate proposals into a workable construct. This construct must effectively manage AWS, promote innovation, function domestically, and have a realistic chance of garnering international support (see figure 1).

II. Background

A. Autonomous Weapons Systems

The US Department of Defense (DoD) Directive 3000.09 (Autonomy in Weapon Systems) defines an autonomous weapon system as:

A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised [AWS] that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.[5] (see figure 2)

The DoD definition requires substantial unpacking to ensure a common understanding of these systems. First, United States Army Lieutenant Colonel

[3] Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. Pa. L. Rev. 1347, 1366, May 2016 (citing Robert H. Latiff & Patrick J. McCloskey, **With Drone Warfare, America Approaches the Robo-Rubicon**, WALL ST. J. (Mar. 14, 2013, 7:37 PM), http://www.wsj.com/news/articles/SB10001424127887324128504578346333246145 [https://perma.cc/C67E-SKNP]).

[4] Jeffrey S. Thurnher, (2012). No one at the controls: Legal implications of fully autonomous targeting. Joint Force Quarterly, 67(4), http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_77-84_Thurnher.pdf .Jeffrey S.Thurnher, 'The Law That Applies to Autonomous Weapon Systems' (American Society of International Law 2013) 17 Insights <www.asil.org/insights/volume/17/issue/4/law-applies-autonomous-weapon-systems>. Michael Schmitt and Jeffrey S. Thurnher, ' "Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 4 Harvard National Security Journal 234 http://harvardnsj. org/2013/05/out-of-the-loop-autonomous-weapon-systems-and-the-law-of-armed-conflict/. Alan Schuller, At the Crossroads of Control: the Intersection of Artificial Intelligence in Autonomous Weapons Systems with International Humanitarian Law, Harvard National Security Journal Vol. 8. 2017. <https://harvardnsj.org/wp-content/uploads/sites/13/2017/02/Schuller-NSJ-Vol-8.pdf.

[5] Department of Defense Directive 3000.09, "Autonomy in Weapon Systems," May 8, 2017, 13 [hereinafter DoDD 3000.09]. [Unites States references are primarily used in this paper because the U.S. is a world leader in autonomous technology and its references are publicly available.]

Christopher Ford, an AWS expert deduced, "autonomy is less a technology as it is a capability comprised of multiple technologies."[6] Therefore, any proposed legal framework will have to address the full spectrum of autonomous capabilities across varied and distinct domains, missions, and platforms. Second, many commentators and international organizations differentiate between autonomous weapon systems (AWS) and lethal autonomous weapon systems (LAWS).[7] The distinction between AWS and LAWS is not the byproduct of autonomy or the inadequacy of the current legal framework, but rather the innate human desire to recognize heightened moral, ethical, and legal implications when the loss of human life is a factor. If an autonomous system possesses lethal capabilities, those capabilities will feature prominently in the LOAC analysis, but there is no requirement for a bifurcated regulatory regime. Therefore, recognizing this distinction independent of the Law of Armed Conflict (LOAC) framework is not necessary; the application of the LOAC principles already account for the difference between a non-lethal and a lethal weapon system. This paper will focus on AWS generally.

Autonomy is not binary; it is a capability that exists on a spectrum of varying degrees (see figure 2). A variety of frameworks have been developed to navigate the various levels of semi-autonomy. The simplest framework to conceptualize is based on Colonel John Boyd's ubiquitous observe, orient, decide, act (OODA) loop.[8] A "human-in-the-loop" system is capable of autonomously selecting targets but will only execute once approval from a human operator is granted.[9] A system that will complete a task unless a human intervenes is a "human-on-the-loop" system, and a system that, once activated, a human can no longer intervene is a "human-out-of-the-loop" system.[10] This paper will explore the legal framework applied to AWS as

[6] Lieutenant Colonel Christopher M. Ford, *Autonomous Weapons and International Law*, 69 S. Car. Law Rev. 413, 416 (2017).
[7] Daniel S. Hoadley and Nathan J. Lucas, *Artificial Intelligence and National Security,* The Congressional Research Service, April 26, 2018, https://fas.org/sgp/crs/natsec/R45178.pdf, 12.
[8] See John R. Boyd, *Destruction and Creation (PDF),* September 3, 1976, U.S. Army Command and General Staff College, https://globalguerrillas.typepad.com/JohnBoyd/Destruction%20and%20Creation.pdf.
[9] See Paul Scharre, *Autonomous Weapons and Operational Risk*, Washington: Center for a New American Security, 2016, https://search-proquest-com.lomc.idm.oclc.org/docview/1834992075?accountid=14746, 43; and Amitai Etzioni PhD, and Oren Etzioni PhD, "Pros and Cons of Autonomous Weapons Systems," *Military Review* 97 (3) 2017, https://search-proquest-com.lomc.idm.oclc.org/docview/1922376987?accountid=14746, 78 (citing Bonnie Docherty, *Losing Humanity: The Case against Killer Robots* (Cambridge, MA: Human Rights Watch, 19 November 2012), https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots, 2).
[10] See Scharre, *Autonomous Weapons*, 43; and Etzioni & Etzioni, 78 (citing Docherty, *Losing Humanity*, 2).

defined above; that is, weapon systems that have the capability to operate with a human "on-the-loop" or a human "out-of-the-loop" (see figure 2).

AWS are distinguishable from both unmanned systems and automatic weapons. In unmanned systems, the weapon is merely an extension of the operator—albeit an extension that can now employ an astonishing combination of standoff and lethality. While the decision to employ force no longer needs to be co-located with the weapon system, legal, moral, and ethical accountability for unmanned systems falls on the decision-makers and is adequately addressed by the existing regulatory landscape.

Automatic weapons are capable of being triggered without a human decision after employment but are rule-based and passive in nature (e.g., land mines, booby traps, improvised explosive devices, etc.).[11] Automatic weapons follow a programmed script in which every outcome is predetermined by a programmer.[12] In an autonomous weapon system, the script contains unprogrammed improvisation space in which no outcome has been predetermined.[13] Dr. Rebecca Crootof, a leading AWS scholar, succinctly describes the difference between automated weapon systems and AWS: "automated weapon systems merely react to triggers, autonomous weapon systems process information to derive conclusions before responding."[14]

In the near future, AWS will also employ artificial intelligence (see figure 3). Congress has defined artificial intelligence (AI) as: "[a]ny artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance. . . . They may solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action."[15] Current AWS are capable of acting without a human decision-maker, but in the near future they will also be able to create and then

[11] Hoadley and Lucas, *Artificial Intelligence,* 4.
[12] Ford, *Autonomous Weapons,* 420.
[13] Id.
[14] Rebecca Crootof, *The Killer Robots are Here: Legal and Policy Implications*, (2015) 36 Cardozo L. Rev. 1837, 1855.
[15] U.S. Congress, House, FUTURE of Artificial Intelligence Act of 2017, HR 4625, 115th Cong., introduced in House December 12, 2012, https://www.congress.gov/bill/115th-congress/house-bill/4625/related-bills?q=%7B%22search%22%3A%5B%22H.+R.+83%22%5D%7D12/12/2017; and U.S. Congress, Senate, FUTURE of Artificial Intelligence Act of 2017, HR 4625, 115th Cong., introduced in Senate December 12, 2012, https://www.congress.gov/bill/115th-congress/house-bill/4625/related-bills?q=%7B%22search%22%3A%5B%22H.+R.+83%22%5D%7D12/12/2017.

execute their own decision cycles. Any proposed AWS regulatory scheme needs to account for the foreseeable advances in AI technology.

AWS differ from any other weapon systems because eventually they will possess the capability to independently hunt and kill human beings. Appropriate concerns undergird the creation of military-grade apex predators. Even proponents of the technology must recognize the enormous risk inherent in AWS: the systems must differentiate biologically identical targets based on nuanced cultural and behavioral cues. Absent that capability, the machine will turn on its creators. With a common understanding of what constitutes an autonomous weapon system and the instinctual rationale underlying the aversion to this technology, knowledge of the current state of AWS is helpful.

B. Current State of Autonomous Weapon Systems Technology

Many proponents of bans or limitations on AWS incorrectly believe that AWS do not yet exist.[16] AWS have been present on the battlefield for decades, albeit in limited and well-defined roles. Current examples of weapon systems that, under certain circumstances, can independently select and engage targets are:

- The US Phalanx Close-in-Weapon System (CIWS).[17] This system is a radar controlled defensive cannon that protects ships against airborne and surface threats and is capable of operating fully autonomously.[18] Twenty-four allies utilize the phalanx CIWS system and six other nations

[16] See Kelly Cass, *Autonomous Weapons and Accountability: Seeking Solutions in the Law of War*, 48 Loy. L.A. L. Rev. 1017, 1024, Spring 2015; Bradan T. Thomas, *Autonomous Weapon Systems: The Anatomy of Autonomy and the Legality of Lethality*, 37 Hous. J. Int'l L. 235, 237, Spring 2015; Benjamin Kastan, *Autonomous Weapons Systems; A Coming Legal "Singularity"?*, 2013 U. Ill. J.L. tech. & Pol'y 45, 50; Shane R. Reeves, and William J. Johnson, *Autonomous Weapons: Are You Sure these are Killer Robots? Can we Talk about it?*, The Army Lawyer,25-31, April 2014 https://search-proquest-com.lomc.idm.oclc.org/docview/1540957074?accountid=14746, 25; China, *Position Paper*, Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, April 9-13; and Gregory P. Noone and Diana C. Noone, *The Debate over Autonomous Weapons Systems*, Case Western Reserve Journal of International Law 47, no. 1 (Spring 2015): 29, http://scholarlycommons.law.case.edu/jil/vol47/iss1/6/, 35.

[17] Brian K. Hall, "Autonomous Weapons Systems Safety," *Joint Force Quarterly:* 86, July, 2017. https://search-proquest-com.lomc.idm.oclc.org/docview/1916950387?accountid=14746, last retrieved December 17, 2018, 89; and Crootof, *War Torts*, 15.

[18] The Phalanx CIWS system usually has a human in-the-loop; however, when it is in "casualty mode," the system is capable of fully autonomous operation. See Kastan, *Autonomous Weapons Systems,* 5.

employ a similar capability;[19]

- US counter-rocket, artillery, and mortar land-based phalanx weapon system (LPWS).[20] This system consists of the radar array (C-RAM) and a kinetic cannon. This system is employed defensively;[21]

- The Israeli Iron Dome is an anti-mortar/missile defense system.[22] This system is the Israeli equivalent to the US's Phalanx/CIWS and LPWS systems;[23]

- The Israeli Harpy Loitering Weapon is an ". . . anti-radar weapon that searches for radars over a wide area and, once it finds them, kamikazes into them."[24] The Harpy can stay aloft for over two hours and operators employing the Harpy do not need to know the specific locations of the enemy radars that will ultimately be targeted;[25]

- South Korea's SGR-A1 (Security Guard Robot). This robot is employed on the 38th parallel and is capable of autonomously locating, targeting, and killing humans that enter the demilitarized zone (DMZ). Despite the fairly extensive precautions and the limited context in which the robot is employed, South Korea still keeps a human in-the-loop;[26]

- The Chinese/Russian PMK-2 encapsulated torpedo mines.[27] These mines can be laid from the air and loiter at depths up to 2000 meters.[28] When a ship or submarine comes within range, the capsule releases a torpedo that tracks and engages the target.[29]

---

[19] See Phalanx Close-in Weapon System, *Raytheon,* https://www.raytheon.com/capabilities/products/phalanx, last retrieved January 17, 2019; and Crootof, *War Torts*, 15.
[20] Hall*, Autonomous Weapons Systems Safety*, 89; and Scharre*, Autonomous Weapons*, 43.
[21] Counter-Rocket, Artillery, Mortar (C-RAM) Intercept Land-Based Phalanx Weapon System (LPWS), US Army, https://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/, last retrieved January 17, 2019.
[22] Crootof, *The Killer Robots*, 15.
[23] Id.
[24] Scharre, *Autonomous Weapons*, 20.
[25] Id.
[26] Christopher P. Toscano, *"Friend of Humans": An argument for Developing Autonomous Weapons Systems*, 8 J. Nat'l Security L. & Pol'y 189, 197; 2015 [subsequent references will include the pin cite to the specific page of the article as it appears in the online version (e.g. 1-82)].
[27] Crootof, *War Torts,* 15.
[28] Scott C. Truver, "Taking Mines Seriously: Mine Warfare in China's Near Seas," *Naval War College Review*, Volume 65, 2012, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1429&context=nwc-review, 12.
[29] See Paul Scharre, *Autonomy, "Killer Robots, " and Human Control in the Use of Force--Part I*, JUST SECURITY,

A responsible inventory of the current state of AWS also requires acknowledgement that advanced weapons development is a non-transparent activity. As such, it is a safe assumption that additional autonomous weapon system capabilities already exist and that at least Russia, China, Israel, and Iran have many more in development.[30] The rapid advancements in AI, robotics, and technology, indicate that AWS are a permanent fixture on the modern battlefield and that the role of these systems will only increase in the future.

C. Employment Considerations of Autonomous Weapon Systems

Critics have argued against the continued development of AWS. The prevailing arguments cite negative ramifications stemming from dehumanizing warfare; insufficient moral, ethical, and legal support for the employment of AWS; and fears of a dystopian future wherein humans become subordinate to AWS. Ultimately, each argument against the development of AWS is flawed.

Arguments Against Continued Development of Autonomous Weapon Systems

The first significant concern with AWS is that removing humans from various aspects of the battlefield will increase the likelihood of war. China and the non-governmental organization Human Rights Watch have both expressed concern that AWS will lower the threshold for war.[31] The argument is predicated on one nation being technologically superior to another to such a degree that the domestic cost of war, in lives and material, is minimal. This argument relies on a flawed assumption. Every bilateral relationship between nations is not solely an economic equation wherein each nation has a threshold price point below which war will automatically be conducted. If this were the state of reality, power disparities would dictate that powerful nations should already prey on less powerful ones.[32] The dehumanization argument ignores the impact of deterrence, alliances, the international order, human

July 9, 2014, *http://justsecurity.org/12708/autonomy-killer-robots-human-control-force-part* .
[30] Toscano, *Friend*, 4.
[31] See China, *Position Paper*; and Bonnie Docherty, "We're Running Out of Time to Stop Killer Robot Weapons," *Human Rights Watch*, April 11, 2018, https://www.hrw.org/news/2018/04/11/were-running-out-time-stop-killer-robot-weapons.
[32] Toscano, *Friend,* 29.

decency, and the myriad other factors present in a society's decision to go to war.[33]

The argument that employment of AWS is morally, ethically, or legally unsupportable collapses as soon as it is tested for validity. Prohibiting development of AWS without allowing for distinctions that recognize the context and manner in which autonomy is employed, leads to suboptimal moral and ethical outcomes. At times, LPWS systems must respond faster than human cognition is capable of perceiving, processing, and reacting. Inserting a human into the LPWS decision loop in those instances negates the utility of the system. Prohibiting the autonomous functions of time-sensitive systems on moral or ethical grounds necessitates the immoral and unethical decision to incur needless death and destruction. It is not morally and ethically superior to permit death and injury from incoming mortars simply because the LPWS system cannot function timely and effectively when a human remains "in-the-loop." As an autonomous weapon advances to the point that it has been validated and verified in certain circumstances as providing superior compliance with the LOAC principles relative to humans, employing humans in these circumstances would be the immoral and unethical option. Superior compliance with the LOAC principles necessarily means fewer military deaths, fewer civilian casualties, and less collateral damage. Last, as the legal "mirror thesis" of law posits, law will adapt and change to reflect the "intellectual, social, economic, and political climate of its time."[34] When national survival becomes contingent on the development, adoption, and use of AWS, the laws associated with the technology will evolve to accommodate the technology.

More than any other factor, western science fiction depictions—the Terminator Effect[35]—appear to drive opposition to the development and use of AWS.[36] Fear that machines may become self-aware and operate independently of all human input is still premature. A Phalanx CIWS system cannot realistically become sentient and commandeer a destroyer, at least

[33] Id.
[34] Brian Z. Tamanaha, *"Law and Society,"* St. John's Legal Studies Research Paper No. 09-0167, 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1345204 ## last retrieved March 16, 2019.
[35] The "Terminator Effect" is a reference to a science-fiction action franchise that has spanned almost 40 years. In the franchise, an artificial intelligence network utilizes robots, called Terminators, to exterminate the human race. The dystopian fears exploited by the franchise are the same ones supporting an international ban on AWS.
[36] Toscano, *Friend*, 2.

not in the near future. While AWS are a long way from that capability, the rate of technological advance, particularly with AI, means that the singularity is closer than it may appear. The fleeting window of time that exists now, provides an opportunity to develop a cogent international AWS framework, which will better enable addressing more difficult and complex systems in the future. Any proposed framework needs to take into account the significant power inherent in autonomy and AI and be flexible enough to adapt in lockstep with technologies. However, autonomous-capable systems are present now, and responsible discussion on the topic requires setting dystopian concerns aside with the realization that, where practicable, humans will remain "in-the-loop" for the foreseeable future.[37]

Arguments for Continued Development of Autonomous Weapon Systems

Arguments in favor of AWS anticipate fewer civilian and military deaths, lower human and material costs in war, superior compliance with the LOAC principles, and a recognition of the inevitability of these systems. Arguably, a benefit to the employment of AWS is fewer military and civilian deaths—at least on an individual engagement basis. The potential for these systems to better comply with the principles of the LOAC is not mere speculation; it is both an inevitability and proposed prerequisite to employment. Removing human factors from various tasks in warfare will lead to more precise outcomes. AWS will be quicker, more accurate, and more effective than humans at an increasing number of battlefield tasks. An autonomous weapon system without a human in the loop will be unimpeded by human factors—emotions, biological limitations, or survival instincts—that inject additional risk into warfare. Additionally, each battlefield task completed by an autonomous weapon system is one that will no longer require risking the lives of servicemembers.

Countries that do not develop autonomous capabilities will be at a military disadvantage, making continued development of these systems an inevitability. The nuclear arms race illustrates this paradigm very well. When the US was the only nation that possessed nuclear technology, all other nations were dependent on the benevolence and judgment of the US not to employ those weapons. Once two nations possessed nuclear weapons, survival of all parties became the impetus to refrain from using nuclear

[37] Id., at 9.

weapons.[38] Rightly or wrongly, only one country has employed nuclear weapons against an adversary and did so when the technology disparity presented a significant military advantage. To maintain parity, it is clear that nations will need to pursue AWS or risk being at the mercy of those that do. The International Committee of the Red Cross recognizes that AWS attract "considerable interest and research funding so such weapons may well be a feature of warfare in the future."[39] Over thirty nations employ or are currently developing autonomous weapon technologies and "[s]tate and non-state actors will certainly pursue such technology since the barriers to entry are much lower, with greater tactical advantages readily available."[40] Despite the current proliferation of AWS, many in the international community are calling for an outright ban.[41]

Source: www.nato.int

[38] Lawrence Freedman, The First Two Generations of Nuclear Strategists, In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, Ed. By Peter Paret (Princeton, NJ: Princeton University, 1986), 738-739.
[39] Toscano, *Friend*, 11 (citing ICRC Resource Center, *Autonomous Weapons: States Must Address Major Humanitarian Ethical Challenges* (Sept. 2, 2013), http://www.icrc.org/eng/resources/documents/faq/q-and-aautonomous-weapons.htm).
[40] Toscano, *Friend*, 12.
[41] See Dan Smith, "Stephen Hawking, Elon Musk Warn of 'Third Revolution in Warfare' with Autonomous Weapons," *ABC Premium News*, Jul 28, 2015, https://search-proquest-com.lomc.idm.oclc.org/docview/1699087903?accountid=14746, December 18, 2018; and William D. Hood, "Autonomous Weapons Systems: What Commanders Should Know," *The Marine Corps Gazette*, March 2015, 43-44.

D. International Ban of Autonomous Weapon Systems

One proposed response to the anticipated problems of AWS is to institute an international ban. Human Rights Watch, the International Committee for Robot Arms Control, and over fifty other non-governmental organizations have advocated for a ban on AWS.[42] One thousand experts and thought leaders, including famous physicist Stephen Hawking, entrepreneur Elon Musk, and Apple co-founder Steve Wozniak, have also advocated for an outright ban on AWS.[43] A ban is problematic for a few reasons. With the currently existing AWS, a ban would require thirty nations to forfeit validated missile defense systems, or require a ban to have exceptions broad enough they would effectively render a ban meaningless. Second, a ban on these systems is predicated on the beliefs (1) that enforcement is possible and (2) the risks of non-compliance are greater than the risks associated with compliance.

Regulating AWS is unlike regulating weapons of mass destruction. Nuclear, chemical, and biological weapons have unique characteristics (e.g. precursor materials; large quantities of rare materials; and specific technologies and equipment for creation, storage, and protection) that render those weapons amenable to international inspection and enforcement. A coercive yet viable inspection and enforcement program targeting autonomy would be impossible. Autonomy is a capability comprised of many technologies.[44] No country would grant the transparency required for effective inspections, and no international agency has the manpower required for enforcement. Setting aside the impossibility of inspection and enforcement, empirical evidence suggests that an outright ban of AWS could lead to worse outcomes.

In their article encouraging open dialogue on AWS, Judge Advocates LTC Reeves and Major Johnson draw on history to explain an apparent contradiction: an outright ban on a nascent weapon system may actually lead to *more* casualties.[45] The theory holds that as new warfighting technology develops, responsible and thoughtful dialogue has the potential to foster appropriate and complementary advances in technology, law, and

[42] Hood, *What Commanders Should Know*, 43-44.
[43] See Smith, *Third Revolution*, indicating that the supporters of this ban have not distinguished between lethal and non-lethal autonomous weapon systems.
[44] Ford, *Autonomous Weapons,* 416.
[45] Reeves and Johnson, *Can we Talk about it?*, 27.

tactics, whereas an outright ban stifles advances in those areas.[46] As more advanced AWS are employed in warfare (an inevitability) a ban will constitute an opportunity cost—time lost in developing technology, law, and tactics.

In 1899, a five-year international ban of balloon-launched projectiles led to significantly more civilian death and destruction during World War II (WWII).[47] Had the ban never been imposed, appreciably better outcomes vis-à-vis the principle of humanity may have been achieved.[48] The outright ban on aerial bombardment effectively tolled all technological development and responsible dialogue on the employment of aerial bombardment.[49] When Allied participation in WWII aerial bombardment became necessary to counter Axis aggression, effective aerial bombardment required indiscriminate obliteration and fire-bombing tactics to generate effects.[50] The technology, applicable legal framework, and tactics were orders of magnitude behind where they could have been if development of the technology and constructive dialogue of the capability had continued unabated.[51] While aerial bombardment technology took almost ninety years to reasonably comply with the LOAC principles, the five years of development lost as a result of the ban translated to avoidable civilian death and destruction in WWII.[52]

The distinction between successful and unsuccessful bans hinges on the difference between a capability and a means.[53] Generally, successful bans prohibit a means but not a capability. A ban on a munition amounts to a nation accepting inefficiency in certain areas in return for the benefits such a regulatory scheme provides their forces (e.g. the banned weapons will not be used against their forces or civilians). Nations that agree to such a ban do not

[46] Id.
[47] See Id., at 28 (Twenty-four countries agreed to the original 1899 ban. A subsequent 1907 ban encountered significantly more resistance and was narrower in scope).
[48] Declaration (IV,1), to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons, and Other Methods of Similar Nature, *The Hague*, 29 July 1899, https://ihl-databases.icrc.org/ihl/INTRO/160?OpenDocument.
[49] Reeves and Johnson, *Can we Talk about it?*, 28.
[50] These techniques were most famously applied to London, Dresden, and Tokyo.
[51] Reeves and Johnson, *Can we Talk about it?*, 28-29.
[52] Id., at 29.
[53] See Law of Armed Conflict Deskbook, 5th Ed. *The Judge Advocate General's Legal Center and School,* 2017, http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2015.pdf, 152 [hereinafter, Deskbook], (hollow-point bullets, frangible rounds, and fragmentation rounds); Deskbook 151, (glass rounds); Deskbook, 159, (chemical weapons); and Deskbook, 20, (biological weapons).

forfeit the ability to utilize a capability, but rather forfeit the ability to use a specific type of munition (means). The successful bans on hollow-point rounds, glass rounds, poisoned rounds, chemical, and biological weapons adhere to this capability/means distinction.[54] Nations accept inefficiencies inherent in inferior means to accomplish objectives as a matter of comity and humanity while preserving the overall capability. An indiscriminate ban on aerial bombardment attempted to eliminate a capability and it failed. AWS represent a capability with different degrees of autonomy; different processes employing autonomy; different autonomous functions, means, and missions; across all domains and platforms. The largest obstacle to a ban is highlighted by the inherent inability to answer the operative question, "ban what?" Until that question can be definitively answered in the narrower context of means, a ban will fail.

The United States has officially stated its opposition to a ban on AWS at the United Nations, "[r]ather than trying to stigmatize or ban such emerging technologies in the area of lethal autonomous weapon systems, States should encourage such innovation that furthers the objectives and purposes of the Convention."[55] Currently, twenty-six countries support a ban, and five, including France, Israel, Russia, United Kingdom, and the United States, outright oppose one.[56] Without those five nations, an effective international ban is unlikely to be enacted. While nominally supporting a ban, China has hedged by officially stating on the record at a UN meeting on AWS, "there should not be any pre-set premises or prejudged outcome which may impede the development of [artificial intelligence] technology."[57]

Last, civil-military considerations related to autonomy will also drive adoption of AWS. There is an inflection point at which market forces require businesses to automate. This point occurs when the cost to automate is comparable to the cost of labor and the quality and quantity of output can equal or exceed that of a human workforce. Businesses that do not automate at this inflection point will lose profits and market share to those that do.

[54] See Deskbook, pp 20, 151, 152, and 159.
[55] United States of America, "Humanitarian Benefits of Emerging Technologies in the Area of Lethal Autonomous Weapon Systems," *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*, April 9-13, 2018, 6.
[56] Tucker Davey, "Lethal Autonomous Weapons: An Update from the United Nations," April 30, 2018, https://futureoflife.org/2018/04/30/lethal-autonomous-weapons-an-update-from-the-united-nations/.
[57] China, *Position Paper*, 2.

Autonomous vehicles are already a reality on the battlefield. Autonomous vehicles are capable of following logistics trains and unmanned helicopters are capable of delivering supplies.[58] Domestically, autonomous cars are on the horizon with millions of autonomous miles logged and active testing programs in Silicon Valley, CA; Phoenix, AZ; and Pittsburgh, PA.[59] In short order, an outright ban of AWS would be wholly incompatible with a society that promotes private sector automation and allows automated systems to assume more and more domestic and non-combat battlefield tasks. Such a modern society will demand the use of AWS to spare the blood of its youth.

III. Autonomous Weapon Systems and Current Law

A. Weapons Law

Article 36 of Additional Protocol I to the Geneva Convention requires nations to conduct a legal review of new weapons, means, or methods of warfare to ensure that their employment will not be prohibited by international law.[60] A weapon review is concerned primarily with two things: avoiding unnecessary suffering and preventing weapons that are indiscriminate or unlimited in scope.[61] Weapons violate this Article when they inflict damage beyond what is necessary for a military objective (e.g. hollow-point projectiles, poisoned weapons, glass projectiles, etc.).[62] Indiscriminate weapons are incapable of being used in a manner in which the proponent can reasonably distinguish between civilian and military targets (e.g. chemical weapons).[63] Biological weapons are an example of weapons that

[58] See Ryan Felton, "Lockheed Martin's Autonomous Military Vehicles Aim To Save Lives In A Different Way," *FoxtrotAlpha,* February 18, 2017, available at https://foxtrotalpha.jalopnik.com/lockheed-martins-autonomous-military-vehicles-aim-to-sa-1792128164; and K-Max, Lockheed Martin, available at https://www.lockheedmartin.com/en-us/products/k-max.html, last retrieved March 16, 2019.

[59] See Aaron Aupperlee, "5 Reasons Pittsburgh is Still Tops in Autonomous Vehicles," *The Pittsburgh Tribune-Review*, July 21, 2017, http://www.govtech.com/fs/5-Reasons-Pittsburgh-is-Still-Tops-in-Autonomous-Vehicles.html; and Ryan Randazzo, "Waymo announces 'Waymo One,' but self-driving ride service isn't public — yet," *Arizona Republic,* December 5, 2018, https://www.azcentral.com/story/money/business/tech/2018/12/05/waymo-one-launches-self-driving-car-service-arizona/2114688002/.

[60] The US signed but did not ratify Additional Protocol I but recognizes Article 36 as customary international law and conducts legal reviews of all new weapons systems. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[61] See Int'l Comm. of the Red Cross, Weapons that May Cause Unnecessary Suffering or Have Indiscriminate Effects (1973), *http://www.loc.gov/rr/frd/Military_Law/pdf/RC-Weapons.pdf*.

[62] Toscano, *Friend*, 17.

[63] Deskbook, 137.

are unlimited in scope: once unleashed, the effects cannot be controlled. As a result, they are unlawful under Article 36.[64]

In the context of Article 36, the distinguishing feature of AWS is the autonomy—the methods and processes by which the AWS selects and authorizes target engagement—not the means with which the AWS engages those targets. As a result, an autonomous system that utilizes chemical, biological, or glass projectiles would be *per se* illegal; whereas, an autonomous system that utilizes an internationally accepted munition would not be precluded by Article 36. Significant advances in AI might eventually pose some issues with regard to limiting the scope of an autonomous system once deployed (e.g. an autonomous weapon system that independently and continuously selects and engages targets).[65] Technology has not advanced to this point, but with the proliferation of AI this capability is not as distant as it may seem. To ensure continued Article 36 compliance in this regard, every autonomous-capable system regardless of munition, should have human over-rides to ensure control over the scope of employment. Additionally, common-sense safeguards in AWS architecture and a margin of error discussed below will minimize future risk. In sum, AWS will have some Article 36 implications but Article 36 will not serve as a bar to the development and use of AWS.

Source: www.nato.int

[64] Additional Protocol I, Art. 36, June 8, 1977, 1125 U.N.T.S. 3.
[65] See the plot to W. D. Ricter, *Stealth,* DVD, Directed by Rob Cohen, Los Angeles, Columbia, July 29, 2005.

B. Law of Armed Conflict Principles

Any autonomous weapon system will need to comply with the Law of Armed Conflict. Legal scholars Gregory and Diana Noone note that, "[n]o academic or practitioner is stating anything to the contrary. . . . Simply put, no one would agree to any weapon that ignores LOAC obligations."[66] The LOAC principles are codified in Additional Protocol I (AP I) to the Geneva Conventions and, although not ratified by the US, the US does consider significant portions of the protocols, including the principles, customary international law.[67] These principles are necessity, humanity, proportionality, and distinction.[68]

Under the necessity principle "[a]ttacks shall be limited strictly to military objectives. . . . military objectives are limited to those objects which by their nature, location, purpose . . . offers a definite military advantage." [69] To be lawful, any destruction or seizure of property must be required by the military dictates of the situation.[70] Humanity pertains to civilians, and requires: "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians, and civilian objects."[71] Of vital import to this principle, combatants are required to take all feasible precautions to limit the injury and suffering of civilians.[72] Proportionality recognizes the tension between necessity and humanity and the reality that war is messy. Proportionality prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[73] Proportionality is a subjective determination made by the cognizant commander. In a war crimes context, the proportionality decision is subject to a reasonableness standard.[74] Distinction requires safeguards to ensure the military nature of targets and parties. AP I, Art. 48, states, "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and

[66] Noone & Noone, *The Debate,* 29.
[67] Deskbook, 71.
[68] See Id., at 133-162.
[69] Additional Protocol I, Art. 52(2).
[70] Id.
[71] Additional Protocol I, Art. 57(1).
[72] Id.
[73] Additional Protocol I, Arts. 51(5)(b), 57(2)(a)(iii).
[74] Deskbook, 148.

between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[75]

Prior to approval for autonomous use, an autonomous weapon system capable of operating with a human "on-the-loop" or a human "outside-of-the-loop" should verify and validate compliance with the LOAC at levels superior to humans under the same circumstances. Theoretically, a machine can be made more compliant with the LOAC than a human. There are two complementary means of accomplishing this compliance. The first strategy limits the situations and scenarios in which a weapon system can/will operate autonomously, thereby minimizing the risk of a violation of the LOAC. Second, the algorithms utilized need to produce an error rate within the employment criteria that is lower than the human error rate under the same conditions. Essentially, the context in which the system is used and the programmed script must be sufficiently restrictive to ensure any improvised outcome will be compliant with the LOAC. Once an autonomous weapon system has demonstrated superior compliance relative to humans, the machine will have achieved *de facto* compliance with the LOAC. *De facto* compliance recognizes that a subjective judgment (e.g. the decision to employ force) can be determined objectively by an autonomous system provided a sufficient number and combination of criteria are met. To determine if a violation of the LOAC occurred, a reasonableness standard will be applied by cognizant tribunals.[76] An inverse relationship between the likelihood of an autonomous weapon committing a violation of the LOAC and the reasonableness of the employment of the system exists. The narrower the employment criteria, the more restrictive the algorithms, and the more rigorous the verification and validation of the system, the more reasonable it is to employ the autonomous system.

Narrow Employment Criteria

Narrowing the context and manner in which AWS are employed can significantly increase the likelihood that an autonomous system will comply with the spirit and intent of the LOAC.[77] For instance, employing an autonomous system only in self-defense and against inanimate targets (such as the Phalanx CIWS, LPWS, and Iron Dome systems) eliminates almost all

[75] Additional Protocol I, Art. 48.
[76] Deskbook, 148.
[77] Ford, *Autonomous Weapons,* 429.

humanitarian, proportionality, necessity, and distinction concerns. Destroying imminent aerial military threats (identified by speed, direction, radar signature, etc.),[78] in self-defense, does not generally expose the proponents of those AWS to war crime liability. Tight employment parameters applied to other autonomous capabilities may not effectively generate near total compliance with the LOAC as they do in missile defense systems, but employment parameters can complement sophisticated LOAC algorithms to generate *de facto* compliance. An example of this complementary construct is South Korea's SGR-A1 robot. First, the robot is defensive in nature—it guards the DMZ between North and South Korea against human incursions with lethal and non-lethal munitions.[79] The DMZ is a militarized hellscape 160 miles long and 2.5 miles wide consisting of a significant military presence, land mines, barbed wire, watch towers, obstacles, and signs.[80] Employing the robot in this particular context and manner significantly reduces the likelihood that the autonomous system will engage innocent civilians, non-military targets, or cause disproportionate destruction. While the employment criteria render violations of the LOAC less likely, the SGR-A1 autonomous system still requires additional algorithmic safeguards to ensure the system does not violate the LOAC.[81]

LOAC Algorithms

To complement sufficiently narrow employment constraints, AWS programming must generate compliance with the LOAC at a rate equal to or better than humans under the same circumstances. Proponents of a ban argue that the LOAC principles inherently require human judgment, and therefore a machine will never be able to comply.[82] These arguments fail to recognize the concept of *de facto* compliance. Humans are fallible and make mistakes. These mistakes translate to an error rate. Once an error rate in a given scenario is quantified, an autonomous weapon system's performance can be measured against humans. If the autonomous

[78] Robert H. Stoner, "R2D2 with Attitude: The Story of the Phalanx Close-In Weapons," *NavWeaps*, http://www.navweaps.com/index_tech/tech-103.php, last retrieved January 18, 2019.
[79] Etzioni & Etzioni, 79.
[80] See Demilitarized Zone, Encyclopedia Britannica, https://www.britannica.com/place/demilitarized-zone-Korean-peninsula, last retrieved January 18, 2019.
[81] The SGR-1 is capable of firing non-lethal ammunition, can distinguish a human with his or her hands in the air, and given that there is time for a human to exercise discretion, retaining a human in the loop; and Toscano, *Friend*, 9.
[82] Noone & Noone, *The Debate,* 26; and International Committee for Robot Arms Control, Berlin Statement, October 2010, https://www.icrac.net/statements/.

weapon's error rate is less than humans under similar circumstances, it is reasonable to use the system; if the error rate of the autonomous system is more than a human, employment is unreasonable. In fact, if an autonomous weapon generates a lower error rate than a human operator, the moral imperative is to employ the system.

Proportionality, necessity, and humanity are principles that can often be reduced to quantifiable algorithms. Proportionality is already a mathematical equation that is executed by humans in targeting cells. A commander sets numerical values on a military target and numerical values on collateral damage. When the value of the target exceeds the acceptable amount of collateral damage, it is permissible to prosecute the target. Provided the values assigned to the target and the collateral damage are reasonable, this principle is met. An autonomous weapon system algorithm would simply compute the predetermined values in the proportionality analysis faster and more accurately than a human. This principle also would require an autonomous system have a real-time update capability, whereby a commander can update the subjective values of targets and collateral damage as often as necessary. If an autonomous system with those capabilities has not malfunctioned, liability for a proportionality violation would fall to the commander that assigned unreasonable values on the military target and/or the collateral damage, not with the autonomous system. Preprogrammed military targets and self-defense algorithms will ensure that necessity is met. The Israeli Harpy Missile system is an example of a system pre-programmed to only destroy military targets. The missile will only attack transmitting radars that meet set criteria.[83] This constraint ensures that any target, while not identifiable at the deployment of the system, is military. Effectively, the pre-programmed script narrows any improvised autonomous action by the Harpy system to targets that satisfy the necessity principle. Similarly, the factors vital to the humanity principle can often be quantified and programmed for optimal results. For example, AWS can be programmed to strike a target based on both pattern of life data and real-time assessments to minimize civilian casualties. These are the very same considerations used now for non-AWS strikes. Additionally, a human must often assume self-preservation risk when assessing whether to engage a target; AWS remove

[83] Israel Aerospace Industries, *Harpy NG*, http://www.iai.co.il/Sip_Storage//FILES/5/41655.pdf, last retrieved February 12, 2019.

emotion and self-preservation risk from the equation, leading to better humanitarian outcomes.[84]

Commentators have called distinction, "the greatest hurdle to the legal deployment of AWS."[85] The perceived difficulty of this hurdle stems from the fact that technology has not yet achieved the capability to appropriately distinguish between combatants and civilians in most scenarios. This reality does require real-time human decision making in most cases, but that may change as technology advances. While certainly challenging, it is feasible that over time narrow and complementary employment constraints, sufficiently robust sensors, AI technology, and appropriate algorithms will be able to achieve *de facto* distinction over broader employment scenarios.

De facto distinction is best illustrated via analogy. A South Korean human sentry tasked with guarding the DMZ between North and South Korea must comply with the principle of distinction.[86] As a baseline, the likelihood that a non-combatant would disregard all posted warnings and attempt to navigate military obstacles and mines in the DMZ is low; therefore, the simple presence of someone in the DMZ already provides the sentry with significant information that aids in the distinction calculus. Next, if an individual is in the DMZ, wearing a North Korean military uniform, carrying a firearm, and does not have his arms raised, a viable case for distinction is satisfied and the decision to engage the target is likely reasonable.[87] The reasonableness of the engagement does not change if the engagement is the result of human judgment or an algorithm. This statistical capability is *de facto* distinction—stacking a sufficient number of required conditions prior to engagement that the autonomous weapon system has a demonstrated error rate lower than a human.

While the South Korean sentry/autonomous system example only paired a narrow employment envelope with three requisite conditions, additional distinction criteria and parameters could be programmed to increase the ability to distinguish combatants and lower the error rate. The number of if/then statements that can be programmed into AWS are limited only by the capability of the sensors. However, for humans, the limitation is the tension

[84] Frank Sauer, "Stopping 'Killer Robots': Why Now Is the Time to Ban Autonomous Weapons Systems," *Arms Control Today*, October 2016, 9.
[85] Kastan, *Autonomous Weapons Systems,* 14.
[86] Additional Protocol I, Art. 48.
[87] Additional Protocol I, Art. 48.

between the personal risk to the warfighter and the number of conditions that must be met prior to the employment of lethal force. While far from perfect, rules of engagement try to navigate this tension between the acceptable amount of risk and the application of lethal force. AWS—free of the strictures of self-preservation, fear, revenge, emotion, and biological constraints—can assume far more risk than what would be acceptable to impose on, or expect of, a human prior to the employment of lethal force (e.g. enhanced escalation of force procedures, voice commands, non-lethal ammunition, de-escalation procedures, etc.). Theoretically, an autonomous weapon system could execute an extremely complex decision tree comprised of thousands of if/then statements in a fraction of a second. Once an autonomous system has demonstrated the capability to outperform humans, *de-facto* distinction has been achieved and a human "in-the-loop" is no longer necessary for compliance with this principle of the LOAC.

For an autonomous system to be employed, validation and verification of the system should confirm that, when employed as designed, the system is superior to a human operator in adhering to the LOAC principles. While discussion of potential testing protocols and strategies is beyond the scope of this paper, it is important to note that the design, execution, and verification of valid autonomous system tests will be a complex and difficult task.[88] However, the difficulty in designing and implementing effective testing will not absolve the sponsor of liability under the LOAC or remove the requirement to verify and validate the efficacy of the system. Today, AWS technology is not advanced enough to outperform humans in most applications or across broad scenarios. A regulatory scheme should be in place before technology advances to the point that broader *de facto* compliance is possible.[89]

Underlying Ethical Architecture

The underlying architecture is a system of constraints, restraints, and defaults to which AWS algorithms and AI must comply.[90] In his book,

[88] Ford, *Autonomous Weapons,* 457-460.

[89] See "AI is a rare case where I think we need to be proactive in regulation than be reactive."—Elon Musk (Catherine Clifford, 9 of the most jaw-dropping things Elon Musk said about robots and AI in 2017, *CNBC,* December 18, 2017, https://www.cnbc.com/2017/12/18/9-mind-blowing-things-elon-musk-said-about-robots-and-ai-in-2017.html).

[90] Isaac Asimov's Three Laws of Robotics espoused in his science fiction book, *I, Robot*, provide an example of a simplistic but broadly-applicable underlying ethical architecture: 1) A robot may not injure a human being or, through inaction, allow a human being to come to harm. 2) A robot must obey orders given it by human beings except where such orders would conflict with the First Law. 3) A robot must protect its own existence as long

Governing Lethal Behavior in Autonomous Robots, Ronald Arkin proposes a detailed and layered ethical architecture for autonomous weapons.[91] Three parts of his ethical decision matrix apply at the operating system level: the ethical governor, the ethical behavior control, and the ethical adaptor.[92] The ethical governor requires an autonomous system to execute non-lethal decision loops for validity after engagement criteria are met but prior to prosecuting the target.[93] This safeguard ensures that a viable non-lethal option does not exist prior to engagement—ensuring that lethality is a last resort. The second element of the ethical decision matrix is an ethical behavior control that limits a lethal response to inside an acceptable ethical framework.[94] The third is an ethical adaptor that permits AI to create a more restrictive ethical framework but never authorizes expansion.[95] Essentially, AI may employ additional "learned" criteria prior to engaging a target, but AI may never disregard pre-set parameters to expand permissible decision space or change a system's initial charter.

The ethical behavior control provides the largest opportunity for ensuring ethical and legal employment of AWS. The platform-specific behavior control systems should be hashed out by the military, experts, ethicists, and other stakeholders on a case-by-case basis. However, some common-sense ethical behavior controls should be included in the underlying architecture of all AWS such as a "do not engage default" that must be affirmatively overridden by precise compliance with all engagement criteria.[96] This default should also be executed whenever the system malfunctions, suffers damage, or a sensor breaks.[97] Pre-programmed self-destruct, self-deactivation, or self-neutralization mechanisms should also be included.[98] Ethical behavior controls are an area ripe for international dialogue, codification, and agreement. Even in the absence of international agreement, the United

---

as such protection does not conflict with the First or Second Law. See Isaac Asimov, *I, Robot*, (Garden City, NY: Doubleday, 1950), 40.

[91] Ronald C. Arkin, Governing Lethal Behavior in Autonomous Robots (2009), 125.

[92] Id.

[93] Id.

[94] Id.

[95] Id.

[96] See Kastan, *Autonomous Weapons Systems*, note 71, 8; and Toscano, *Friend*, 20.

[97] "Do not engage" defaults are consistent with US military practice vis-à-vis non-autonomous weapon systems. For example, an observer can send an artillery mission as "do not load." This means that required data is generated, but the weapon is not loaded and cannot fire. To fire the mission, the observer must send the message "cancel do not load," and the mission becomes active.

[98] Crootof, *The Killer Robots*, 43.

States should consider implementing domestic regulation requiring ethical behavior controls in all AWS.

Control Measures

Once an autonomous system is approved for use, there must be clearly defined parameters under which the autonomous system is verified and validated. Responsible use of AWS will then include control measures that provide a margin of safety. A margin of safety further narrows the employment window and reduces risk.[99] These additional parameters will be customized to each autonomous system based on the individual system's design and functions. For instance, limiting a geographic maneuver box, capping the amount of time an autonomous system may operate independently, limiting payloads, limiting fuel, and withholding approval authority to a higher commander are all reasonable controls that could be placed on an autonomous weapon system to ensure a margin of safety.[100] This concept is also consistent with current practice. Many nations have universal safety rules (e.g. "never point a weapon at anything you do not intend to shoot") but also has weapon-specific safety criteria to fill gaps in the general rule created by the particularities of a weapon (e.g. check the back-blast area before using a shoulder-fired rocket).

C. US DoD Directive 3000.09 (Autonomy in Weapon Systems)

DoD Directive 3000.09, last updated May 8, 2017, currently implements many constraints and restraints relative to the development of AWS. First and foremost, humans must be "on-the-loop" for AWS that provide defense of manned installations and platforms—humans must be "in-the-loop" for all other AWS.[101] Next, all systems must be verified and validated through a rigorous testing and evaluation process.[102] The employment of these systems will be limited to a reasonable period of time, and three safeguards are required to prevent unanticipated consequences including an adversary

[99] Margin of safety, "the margin required in order to ensure safety; in engineering the margin of safety is the factor of safety (strength of the material divided by the anticipated stress) minus one." Ronald A. Beaulieu, "*Margin of Safety Definition and Examples used in Safety Basis Documents and the USQ Process,*" https://www.osti.gov/servlets/purl/1134068/, last retrieved February 13, 2019.
[100] See e.g. International Committee for Robot Arms Control, *Berlin Statement*, October 2010, https://www.icrac.net/statements/.
[101] DODD 3000.09 4 a and 4 c 2 (a) & (b).
[102] DODD 3000.09 4 a 1.

hijacking the system.[103] To ensure an autonomous weapon system works as intended, system hardware must have appropriate user interfaces, user-friendly controls, pertinent safeties, anti-tamper measures, clear activation/deactivation procedures, and traceable feedback capabilities.[104] DoDD 3000.09 also ensures AWS employment complies with, ". . . law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement."[105] Additionally, offensively-employed AWS must be designed to disengage when communications are degraded.[106] An autonomous system designed to function outside the parameters of the Directive requires Under Secretary of Defense approval at both the development and fielding stages.[107] Last, the regulation addresses sales and transfers of AWS technology.[108]

IV. Accountability

Accountability is another essential safeguard against violations of the LOAC. Accountability enables punishment and promotes deterrence, two interrelated concepts that shape the decisions and behavior of individual actors. Some legal theorists posit that violations of the LOAC by AWS do not present accountability problems.[109] They cite unanimous consent among lawyers that, ". . . anyone who commits a LOAC violation should be held accountable (i.e. in [an] AWS scenario that may be the system programmer) and anyone in a superior/command position who knew or should have known about the violation may be held accountable as well."[110] This is a logical leap. This position is correct in every case where intent and/or negligence on the part of a stakeholder exists. The programmer that intentionally programs malicious code into the system, the commander that intentionally employs the autonomous system outside the verified scenarios, and the negligent autonomous system "on-the-loop" supervisor that did not intervene when he had a duty to do so, all provide a clear and direct path to legal liability for violations of the LOAC. Deeper analysis reveals a potential gap in accountability that occurs when (1) there is a violation of the LOAC;

[103] DODD 3000.09 4 a 1 (a), (b), & (c).
[104] DODD 3000.09 4 a 2 (a) & (b) and 3 (a), (b), (c).
[105] DODD 3000.09 4 b.
[106] DODD 3000.09 4 c 1.
[107] DODD 3000.09 4 d.
[108] DODD 3000.09 4 e.
[109] Noone & Noone, *The Debate,* 30-31.
[110] Id., at 31.

(2) the violation is the result of an unforeseen autonomous weapon system malfunction; and (3) no stakeholder has the requisite *mens rea* for personal accountability.[111] The commander, the deployer, the programmer, the contractor, and the manufacturers of the various sensors have all been proposed as individuals that could or should shoulder responsibility in the event of such an autonomous system malfunction.[112]

A. Commanders

Many have proposed holding the commander responsible if an autonomous weapon system "goes rogue."[113] This option is suboptimal and would hold a commander responsible for actions over which he had no control simply by nature of his command position. If an autonomous system is able to pass the approval crucible and is employed within the defined parameters and approved scenario, the autonomous system would have demonstrated superior compliance with the LOAC principles relative to humans. If commanders are forced to assume liability for the employment of AWS, they are incentivized *not* to employ the system despite its validated superiority. This perverse incentive structure is a moral temptation: a tension that exists when there is a right thing to do, but competing interests provide justification not to do it.[114] If an autonomous system provides better compliance with the LOAC, the "right" thing to do is to utilize the system. Holding commanders criminally or administratively responsible when they do not act intentionally or negligently has the second-order effects of less compliance with the LOAC principles and stifling military innovation. Additionally, such a liability scheme is not consistent with customary interpretations of command responsibility.[115]

---

[111] Crootof, *War Torts*, 9.
[112] Id., at 14.
[113] Toscano, *Friend*, 28.
[114] Rebecca J. Johnson, Moral Decision Making, October 1, 2015, Slide 8 Notes, Lecture delivered October 9, 2018.
[115] See Deskbook, 185 (Citing *U.S. v. Tomoyuki Yamashita* (1946), "The commander's personal dereliction must have contributed to or failed to prevent the offense" and *The United States of America vs. Wilhelm von Leeb, et al., US Military Tribunal Nuremberg, Judgment of 27 October 1948,* "Military subordination is a comprehensive but not conclusive factor in fixing criminal responsibility . . . A high commander cannot keep completely informed of the details of military operations of subordinates . . . He has the right to assume that details entrusted to responsible subordinates will be legally executed . . . There must be a personal dereliction. That can only occur where the act is directly traceable to him or where his failure to properly supervise his subordinates constitutes criminal negligence on his part. In the latter case, it must be a personal neglect amounting to a wanton, immoral disregard of the action of his subordinates amounting to acquiescence. Any other interpretation of international law would go far beyond the basic principles of criminal law as known to

B. Contractors

Others have suggested domestic product liability law fill the accountability gap.[116] This proposal is problematic. Carried to its logical conclusion, no company would manufacture weapons of war if it could then be held liable for the use of those weapons. Nations need weapons for survival and modern necessity dictates those weapons be produced by industry. The solution to this tension is to grant domestic immunity for weapons contractors—precisely the state of the law in the US. In *Boyle v. United Technologies Corp*.,[117] the US Supreme Court held "liability for design defects in military equipment cannot be imposed, pursuant to state law."[118] The government contractor defense holds that liability is not appropriate when: "(1) the United States approved reasonably precise specifications; (2) the equipment conformed to those specifications; and (3) the supplier warned the United States about the dangers in the use of the equipment that were known to the supplier but not to the United States."[119] Imposing liability on contractors for AWS employment would stifle military innovation and create a system in which a nation would be incapable of defending itself. Since autonomy is a capability that is applicable across myriad domains, platforms, and munitions, an exception to domestic product liability for AWS employment will necessarily be so broad that it would subsume the general rule. Imposing liability on contractors leads to the inevitability of industry withdrawing from weapons production or exorbitant costs[120]—untenable outcomes for any nation.

C. Programmers

Programmers who do not act intentionally or negligently pose two issues for accountability. The first issue is the government contractor defense. As a subset of contractors, programmers also enjoy the protection of the government contractor legal defense.[121] Second, programming is now generally done in teams. These teams effectively dilute individual liability to

---

civilized nations.")

[116] See Kastan, *Autonomous Weapons Systems*, 19.

[117] *Boyle v. United Technologies Corp*., 487 U.S. 500 (1988).

[118] Id., at 512.

[119] Id.

[120] Id.

[121] See Cass, *Autonomous Weapons*, 23 citing Int'l Comm. of the Red Cross, Report of the ICRC Expert Meeting on "*Autonomous Weapons Systems*: Technical, Military, *Legal* and Humanitarian Aspects', 26-28 March 2014, Geneva 2 (2014), 8 (out of the four *legal* regimes listed, the only one applicable to programmers acting unintentionally is product liability which is subject to the same restrictions as contractor liability).

the point that there is no personal accountability to be had for malfunctions resulting from unintentional programming errors that were not detected in the testing stage.

D. Potential Liability Gap

Who should be responsible if an autonomous weapon system acts outside its prescribed parameters and commits a war crime? Suppose the commander was not negligent, the deployer was following lawful orders; the programmer, manufacturer, and the developers did not act negligently or intentionally and are effectively immune from civil liability under various legal doctrines.[122] In such a scenario, every conceivable stakeholder will lack the requisite *mens rea* for a war crime.[123]

Assuming full compliance with approval processes, directives, and reviews; verification and validation; and proper employment, the potential for a malfunction that leads to an unintended violation of the LOAC, while minimized, still exists. Proponents of AWS do not anticipate perfect systems, just better ones. Therefore when, *not if*, a violation of the LOAC occurs despite proper implementation of all safeguards, there would be no party to hold responsible under current liability frameworks. The remaining entity that can be held responsible for violations of the LOAC by AWS is the state. There is a split between scholars as to whether current international law defaults to state liability or if there is a liability gap. Some scholars have determined that the law eventually defaults to state liability through at least two avenues.[124] However these default paths to state liability are fraught with jurisdictional issues.[125] Other scholars argue that the more difficult cases when no person or entity acts intentionally or negligently, create an "accountability gap."[126] Whether this area of the law only needs jurisdictional reform or an entirely new accountability mechanism, it is an area of US and international law ripe for clarification and specificity.

---

[122] Kastan, *Autonomous Weapons Systems,* 22.

[123] See Crootof, *War Torts*, 24, note 155*, citing e.g.*, Rome Statute, *supra* note 13, art. 30(1) ("[A] person shall be criminally responsible and liable for punishment . . . only if the material elements are committed with intent and knowledge."); *see also* Prosecutor v. Blaškić, Case No. IT-95-14-T, Trial Chamber Judgment, P 152 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 3, 2000), *http://www.icty.org/x/cases/blaskic/tjug/en/bla-tj000303e.pdf* [*https://perma.cc/4FG6-WZRE*] ("[T]he *mens rea* constituting all the [grave breaches of the Geneva Conventions] includes both guilty intent and recklessness which may be likened to serious criminal negligence.").

[124] Ford, *Autonomous Weapons,* 475.

[125] Crootof, *War Torts*, 28.

[126] Id., at 4.

V. Recommendations

A. Proposed Changes to Department of Defense Directive 3000.09 Autonomy in Weapon Systems

A regulatory framework that synergistically limits the decision-space for AWS (and in the future AWS with incorporated AI) will help ensure the responsible development of these systems (see figure (3) for a graphic depiction of systematically limited decision-space). An updated DoDD 3000.09 can serve as a strategic messaging tool to the rest of the world clearly communicating the United States' stance on AWS.[127] Additionally, the Directive can serve as a model that can be utilized as a baseline for determining points of international agreement on many aspects of AWS.

Nuclear Interface

The obvious and missing safeguard from DoDD 3000.09 is a categorical prohibition on any AWS/nuclear interface. AWS should never carry, control, respond to, or target nuclear weapons. The consequences of nuclear weapons are so grave that a human, preferably multiple humans, should remain in nuclear decision loops into perpetuity.[128] Placing this simple safeguard into the regulation also sends a favorable international message. Intentions are never certain in international relations. Prohibiting nuclear/AWS interface is one intention that should unequivocally be broadcast, and ideally, reciprocated.[129] The United States—with its nuclear triad (submarine-launched, land-based and air-delivered nuclear warheads)—would not be required to forfeit second-strike capability[130] with the inclusion of a nuclear prohibition in the Directive.[131] The upside to this action is that international actors with less or no nuclear diversity and therefore higher risk may be more likely to agree to an AWS/nuclear interface ban if the US has already taken that step.

Memorializing

[127] Freedman, *Nuclear Strategists*, 754.
[128] Ashley Deeks, Noam Lubell, & Daragh Murray, Daragh, "Machine Learning, Artificial Intelligence, and the Use of Force by States," 10 J. Nat'l Security L. & Pol'y __ (forthcoming 2019).
[129] Freedman, *Nuclear Strategists*, 754.
[130] Id., at 753.
[131] U.S. Department of Defense, *Nuclear Posture Review,* Office of the Secretary of Defense Washington, DC: Pentagon, February 2018, 42.

AWS must be capable of recording and storing the external stimuli and objective criteria relied on to carry out the autonomous functions of the systems. While this seems similar to traceable feedback,[132] the clause should be strengthened and clarified—if a system is capable of operating without a human in-the-loop, humans need to be able to evaluate the efficacy of the loop. Such a recording of inputs will provide for continuous process improvement, accountability, and justification. Additionally, a recording will also allow for the reconstruction of accidents, a vitally important capability for assessing liability for malfunctions. Last, and most importantly, recording will ensure these issues do not reoccur.

Stated Policy Preference on Levels of Autonomy

The current Directive does not enumerate an autonomy hierarchy. The Directive should be amended to clearly articulate a policy preference that requires a human "in-the-loop" when practicable, "on-the-loop" when feasible, and only "out-of-the-loop" when an autonomous weapon system will not be able to function effectively under either of the other two modes. Simply because the capability to remove human decision making from the battlefield may quickly become a reality in broader scenarios, does not mean it should be the reality without carefully weighing the alternatives.

Ethical Behavior Control Requirement

DoDD 3000.09 should also include a requirement for an underlying ethical architecture as discussed above. The Directive should merely require the presence of an architecture as a pre-condition to approval of all autonomous weapons. The actual architecture will change as the understanding and regulation of the autonomous capability grows.

Approval Authorities

Last, the Directive should require the AWS approval process assign employment authorization levels commensurate with the missions, capabilities, and risks of each autonomous weapon system. Withholding approval authorities for weapon employment at higher-level commanders with the responsibility, perspective, and experience commensurate with the risks involved is a common safeguard utilized to balance equities

[132] DODD 3000.09 4 a (3) (b).

appropriately. The viability of this safeguard and the appropriate level for its execution should be considered for each AWS.

B. Indemnification

Addressing the shortcomings in accountability law is more complex. Dr. Crootof has proposed an innovative way to ensure a clear path of accountability in the context of AWS. Dr. Crootof proposed "war torts."[133] A war tort would apply when no individual party or entity has the requisite mental state required for criminal liability. In this narrowly-defined category, the country employing the autonomous system would be strictly liable for damages incurred as a result of a violation of the LOAC. A war tort construct serves to indemnify the commander when an autonomous weapon system is employed as designed and approved. Alternative AWS liability frameworks try to impute liability where none exists, reach the same conclusion by default through complex analysis rife with jurisdictional issues, or simply accept the accountability gap. Absent a war tort regime and the accompanying commander indemnification, a perverse incentive exists to utilize warfighting means leading to sub-optimal outcomes under the LOAC in an effort to avoid personal liability for the unforeseeable actions of a machine. A war tort system serves to absolve a commander of liability if technology that enhances compliance with the LOAC is utilized as designed. Indemnification also reinforces robust national verification and validation processes and procedures, encourages reasonable constraints on the employment of AWS, and provides monetary compensation for damages to victims and their families. A war tort regime will also incentivize contractors to ensure their systems behave as intended—or suffer loss of contracts, clawed-back profits, and other economic damages. A war tort regime would be designed to supplement, not supplant, the existing international war crime system.[134] Given the potential benefits of AWS and accountability concerns, there is a realistic chance that many nations will agree to implement a war tort regime as a matter of comity. Additionally, the United States and allies could utilize soft power over time to promote an international war tort regime. The flow chart in figure 1 demonstrates the limited circumstances in which accountability concerns could arise. A war tort regime would provide a limited mechanism of accountability to victims and a clear path to AWS liability.

[133] Crootof, *War Torts*, 28.
[134] Id.

C. International Approach

Three NATO nations oppose a ban of AWS, the US, the UK, and France; therefore, NATO is an international entity that has a realistic opportunity to develop well-reasoned principles and meaningful international consensus on development and employment of AWS.[135] With an AWS ban unlikely, international consensus on many facets of AWS is still be feasible. There have been multiple efforts at producing non-binding manuals on the application of International Humanitarian Law to different aspects of warfare—for example the Tallinn Manual, San Remo Manual, and the Manual on International Law Applicable to Air and Missile Warfare.[136] NATO Allied Command Transformation is uniquely situated to charter and develop a similar manual incorporating the legal, moral, and ethical landscape of AWS based upon its findings in *Autonomous Systems*

Issues for Defence Policymakers.[137] If consensus was reached among the Allies at the North Atlantic Council to accept such a manual, it would go beyond the US executive fiat in DoDD 3000.09 and provide additional room for policy, intent, explanation, and scenarios. A manual that fleshes out the thorny legal issues associated with AWS would provide a NATO standard for the responsible international development and employment of AWS without stifling innovation, investment, and employment of these systems. In time, validated concepts developed as part of this manual may become customary international law and/or be codified in treaties.

Conclusion

The potential benefits and advantages of AWS are significant enough that international consensus on a ban is untenable and, similar to the 1899 ban on aerial bombardment, may be counter-productive long-term. Responsible development and employment of these systems requires a disciplined and reasoned approach to AWS development, as well as changes to national

---

[135] Elizabeth Minor, Prohibiting Autonomous Weapons Systems, OpenDemocracy, London, 23 Apr 2015, 2.

136 See Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013); San Remo Manual on International Law Applicable to Armed Conflicts at Sea (Louise Doswald Beck ed.,1995); and Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare (2009).

137 Autonomous Systems Issues for Defence Policymakers, Andrew P. Williams and Paul D. Scharre, 321 pages, (2014).Capability Engineering and Innovation Division Headquarters Supreme Allied Commander Transformation
Norfolk, Virginia, United States, https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf

law, national policies and international law which the nations of NATO and its partners can pursue to ensure war crime accountability.[138] Nations must require AWS to comply with standard weapons law. Second, prior to approving an autonomous weapon system for use, that system must have demonstrated superior compliance with the LOAC relative to a human operator under similar conditions. Next, the underlying software architecture, regardless of the AWS' platform and capabilities, must have similar fail-safe attributes including a default to restraint, canceling the mission, and/or self-destructing. On top of that architecture, weapon system-specific control measures should further promote compliance with LOAC, such as preprogrammed maneuver boxes, time limits, payload restrictions, and elevated approval authorities. Service regulations and international legal frameworks must criminalize employment of AWS outside of the validated design parameters. All of these measures are capable of unilateral US implementation but are ripe for international review, non-binding guidance, and/or regulation.[139] Last, when an autonomous system violates principles of the LOAC and no individual liability attaches, the country employing the system should be held strictly liable for the damages under a formalized war tort regime.

The proposed legal framework for AWS recognizes the inevitability of AWS and the potential benefits of this technology. The framework ensures compliance with customary international law and encourages responsible AWS development without stifling innovation. Most importantly, this proposal has the potential to garner both domestic and international backing as it complements long-standing principles of war that already enjoy near universal support.

138 Crootof, War Torts, 28.
[139] Crootof, *The Killer Robots*, 44.

Illustrations (provided by the author)

Figure 1

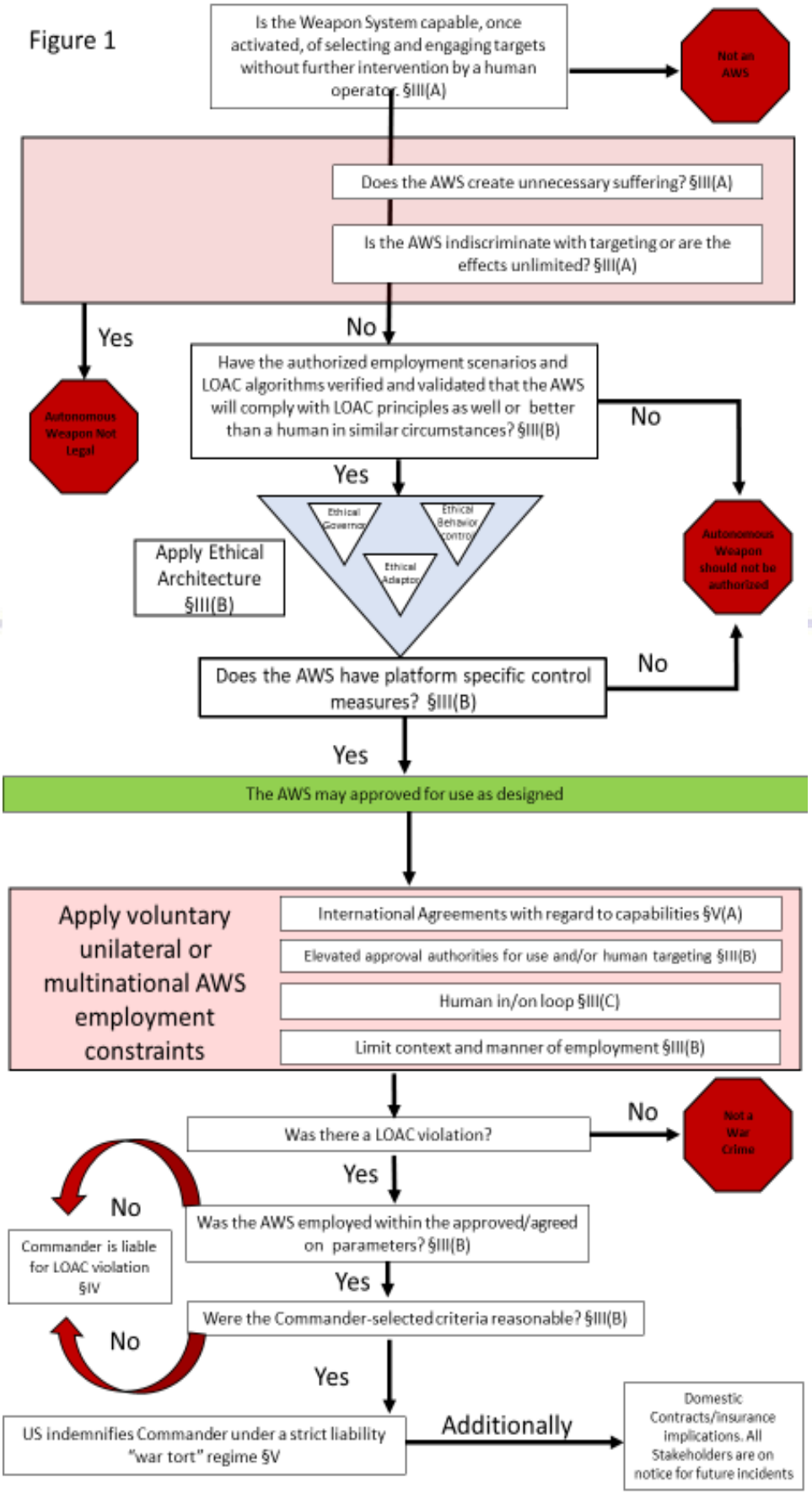


Figure 2

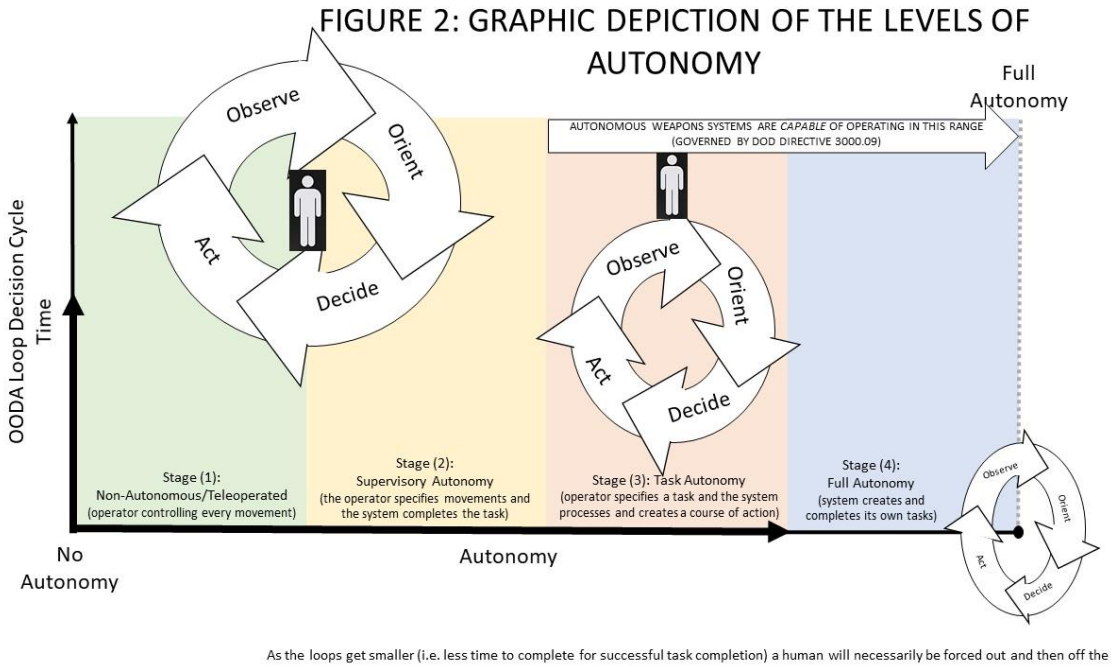
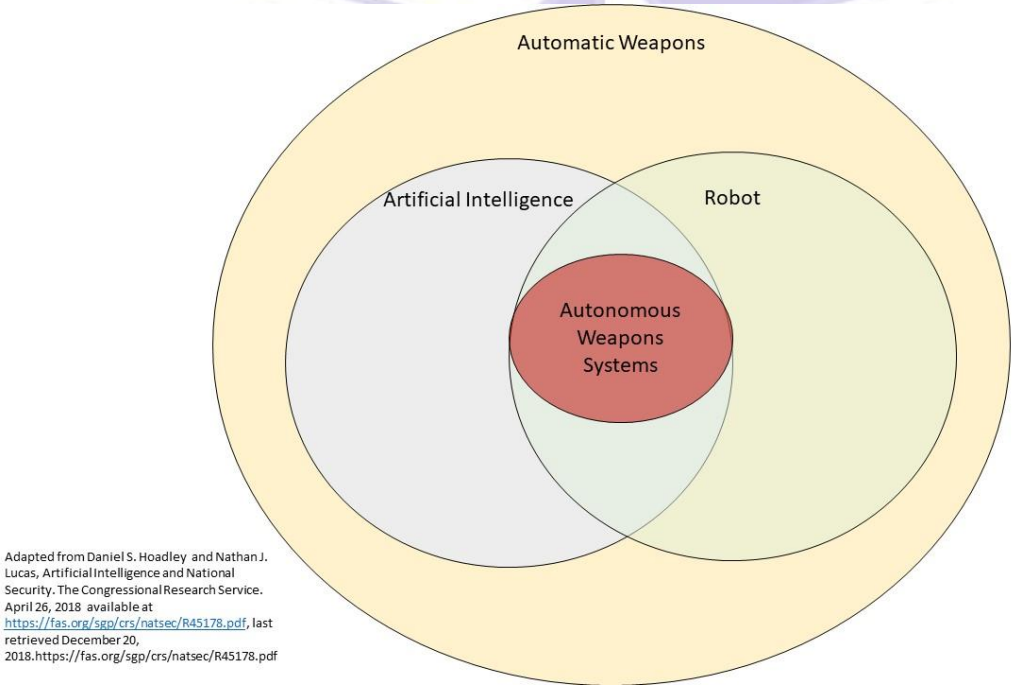
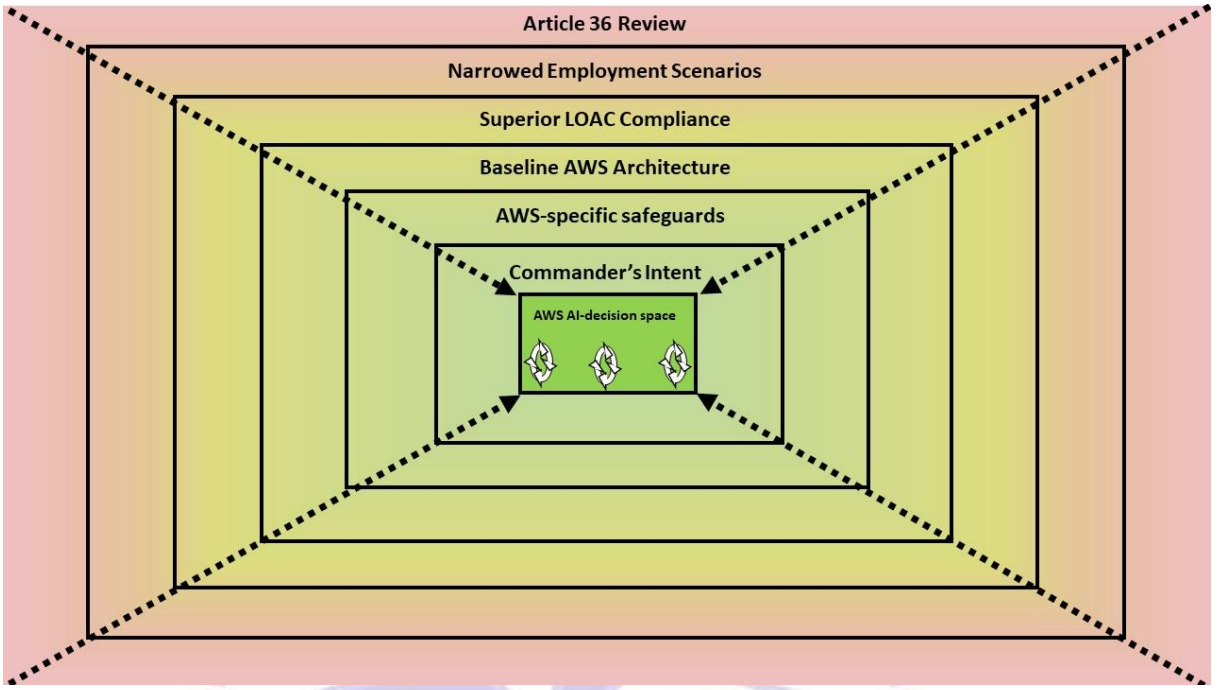


Figure 3



Adapted from Daniel S. Hoadley and Nathan J. Lucas, Artificial Intelligence and National Security. The Congressional Research Service. April 26, 2018 available at https://fas.org/sgp/crs/natsec/R45178.pdf, last retrieved December 20, 2018.https://fas.org/sgp/crs/natsec/R45178.pdf

Figure 4


Article 36 Review
Narrowed Employment Scenarios
Superior LOAC Compliance
Baseline AWS Architecture
AWS-specific safeguards
Commander's Intent
AWS AI-decision space

***

Source: www.nato.int

U.S. Export Controls: The Future of Disruptive Technologies[1]

by Christopher Timura,[2] Judith Alison Lee,[3] R.L. Pratt[4] and Scott Toussaint[5]

Introduction

Export controls administered by the United States and other NATO

[1] The views expressed in this article are solely those of the authors and may not necessarily represent the agreed upon views of NATO, ACO, ACT or Gibson, Dunn & Crutcher LLP.

[2] Christopher Timura is an attorney in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade Practice Group. Mr. Timura helps emerging technology clients across sectors solve regulatory, legal, and political problems that arise at the intersection of national security, trade, and foreign policy. He earned a Juris Doctor and a Ph.D. in Cultural Anthropology at the University of Michigan.

[3] Judith Alison Lee is a partner in the Washington, D.C. office of Gibson Dunn & Crutcher LLP and Co-Chair of the firm's International Trade Practice Group. Ms. Lee practices in the area of international trade regulation, including USA Patriot Act compliance, economic sanctions and embargoes, export controls, and national security reviews.

[4] R.L. Pratt is an associate in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade Practice Group. Mr. Pratt counsels clients on compliance with U.S. economic sanctions, export controls, foreign investment, and international trade regulatory issues and assists in representing clients before the U.S. Departments of State, Treasury, and Commerce.

[5] Scott Toussaint is an associate in the Washington, D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade Practice Group. A former adviser to a member of the U.S. House of Representatives, his practice focuses on compliance with U.S. laws governing international business transactions, including economic sanctions, export controls, and foreign investment in the United States.

Member States restrict the sharing of sensitive goods, services and technology, with significant impacts on NATO's ability to develop and deploy on the battlefield emerging technologies like artificial intelligence-enabled and hypersonic defensive and offensive weapons systems. Indeed, recent export control legislation enacted by the United States—and implementing regulations that are currently being written—will play a major role in determining the NATO community's ability to field interoperable equipment and prevent hostile powers from dominating leading-edge research and development.

On August 13, 2018, President Trump signed into law the most sweeping changes to the U.S. export control regime in decades.[6] Among other things, the Export Control Reform Act of 2018 ("ECRA") modernises the United States' primary authority for export controls on dual-use items (items with both civil and military applications) by requiring the President for the first time to identify and establish both export and foreign investment controls on "emerging" and "foundational" technologies that are essential to national security. The U.S. Department of Commerce has now begun the process of drafting regulations to identify particular "emerging" and "foundational" technologies and to develop corresponding licensing requirements for transfers of these technologies with U.S. allies and adversaries. In addition to new export licensing requirements, any investments, including investments that do not result in foreign person control, in U.S. businesses working with the technologies identified will also be subject to foreign investment review and potential blocking by the Committee on Foreign Investment in the United States ("CFIUS").[7]

How the United States implements these new controls will significantly shape when, where and how disruptive dual-use technologies like artificial intelligence ("AI") and hypersonics ultimately develop.[8] Unilateral implementation of stringent controls on these important new technologies could restrict international cooperation on their development or use, even

[6] *See, e.g.*, Congressional Research Service, 'The U.S. Export Control System and the Export Control Reform Initiative' R41916, (Jan. 28, 2020) 2; Samuel Rubenfield, 'Law Formalizes Export Control Rules' *Wall Street Journal* (Aug. 17, 2018).

[7] CFIUS is an interagency committee authorized to review the national security implications of investments made by foreign companies and persons in U.S. businesses ("covered transactions"), and to block transactions or impose measures to mitigate any threats to U.S. national security.

[8] "Disruptive technology is an innovation that significantly alters the way that consumers, industries, or businesses operate. A disruptive technology sweeps away the systems or habits it replaces because it has attributes that are recognizably superior." Tim Smith, 'Disruptive Technology' *Investopedia* (Mar. 21, 2020).

among close U.S. allies. Application of these new authorities could, for example, hinder the interoperability of important military platforms even among the United States' NATO allies. There is some expectation that the U.S. Department of Commerce may make its efforts to control these technologies multilateral and collaborate with NATO Member States, among other U.S. allies, to impose uniform controls. But there is no guarantee that international agreement can be reached or that the United States will not "go it alone."[9] In fact, the United States has already shown some reluctance to offer favourable treatment for its NATO allies when applying both new and old international trade authorities under U.S. law.[10]

To help members of the NATO community better understand these coming developments, this article proceeds as follows. In Section I, we explain how U.S. export controls work and the policy rationale(s) behind them. In Section II, we provide a high-level overview of recent legislative changes to the U.S. export control regime, and explain the rulemaking process, currently underway, through which the United States will develop controls on so-called "emerging" and "foundational" technologies. In Section III, we describe the various factors, such as whether innovation of a particular technology is centralized or diffuse, that will affect how impactful these new controls are likely to be. Finally, in Section IV, we conclude by illustrating how U.S. export controls are likely to impact two areas of emerging technologies—hypersonics and artificial intelligence—the successful development and deployment of which will likely be critical to NATO's future military capabilities.

I. Background: U.S. Export Controls Explained

As a policy matter, U.S. export controls attempt to balance the needs to protect U.S. national security, support American industry and technological superiority, and permit coordination and exchange with U.S. allies. These controls are rooted in multilateral cooperation that allows for the supply of dual-use goods to allied nations and keeps these items and their underlying technology out of the hands of U.S. adversaries. The Wassenaar Arrangement[11]—the multilateral agreement that underlies much of the Export

[9] *See, e.g.*, Modification of License Exception Additional Permissive Reexports (APR), 85 Fed. Reg. 23,496 (Apr. 28, 2020).
[10] *See, e.g.*, Provisions Pertaining to Certain Investment in the United States by Foreign Persons, 84 Fed. Reg. 50,174, 50,179 (Sept. 24, 2019)
[11] WASSENAAR ARRANGEMENT, 'About Us' (May 30, 2019).

Administration Regulations ("EAR")[12]—grew out of Cold War-era coordination by the NATO nations to restrict the sale and shipment of strategically important, dual-use items to the communist nations closely allied with the Soviet Union. After the Cold War, as NATO's attention shifted, these nations initiated a renewed export control initiative to restrict the proliferation of arms and dual-use items to rogue states and terrorists.[13]

The agreement concluded in 1995 in the city of Wassenaar, Netherlands among these nations is not a treaty and, as such, does not independently have the force of law. The economic and security benefits of a standardized export control system continue to encourage Wassenaar nations to largely maintain multilateral export controls and have encouraged the development of additional international regimes to coordinate export controls, including the Nuclear Non-Proliferation Treaty, the Australia Group Controls, as well as UN Security Council Resolutions. However, there is no overarching legal requirement that these controls remain multilateral. Countries may implement unique, unilateral controls. Straying from the multilateral origins of the current export control regime by imposing unilateral controls, however, may negatively impact technological development, coordination and exchange among NATO allies.

A. What Do They Regulate?

U.S. export controls regulate the provision of U.S.-origin items to other countries or to foreign persons. The United States maintains two primary legal regimes for implementing these controls. The International Traffic in Arms Regulations ("ITAR") apply to certain items designed for and used in military and intelligence applications.[14] The EAR applies to certain military items, items in short supply, and items that may have military and civilian uses—"dual-use" items—a broad category covering almost all items not captured under the ITAR. Although these regimes have important distinctions, there are significant similarities in the scope of items and activities they regulate and the structure of their restrictions.

Items subject to these export control regimes include goods, software, and technology (i.e., information on the development, production or use of

[12] 15 C.F.R. § 730 *et seq*.
[13] In 1995, these nations met in Wassenaar, Netherlands to outline a new trade control regime. Significantly, China did not participate in these initial negotiations and remains outside of the current Wassenaar system.
[14] 22 C.F.R. § 120 *et seq.*

controlled items) that are physically present in the United States, as well as items that were produced in or otherwise originated from the United States.[15] Both export control regimes may also apply to items that are made outside of the United States. Under the ITAR, foreign-made items that incorporate an ITAR-controlled part or component are subject to the same restrictions as that part or component. The ITAR effectively "sees through" the end-item to its ITAR-controlled component and applies those same controls to the end-item. The ITAR also control items made from ITAR-controlled software and technology, the provision of defence services, and the brokering of defence articles and services.

The EAR takes a more permissive approach. Foreign-made items may incorporate a minimal amount of U.S.-origin content (typically 25%) and remain outside the scope of the EAR. However, foreign-made items that incorporate more than that allowable minimum are treated as U.S.-origin items and are subject to the EAR.[16] In certain limited circumstances, the EAR also controls foreign-made items that contain any amount of certain, highly controlled U.S.-origin content or that are the direct product of certain other U.S.-origin technology and software.[17]

Both the ITAR and EAR control the export of the items to which they apply. Under both programs, an export of a covered item must be authorized or exempt from the need for authorisation before the export occurs. Exports not only include the actual shipment or transmission of an item out of the United States, but also include the release of technology to a foreign person, even when that foreign person is physically located in the United States (a "deemed export").[18] For example, emailing design specifications of a controlled item to a French national colleague or discussing with that same colleague the process for using the item is considered an export of that controlled technology.

In addition to controlling the initial export of covered items from the United States, these regimes also restrict the re-export and transfer of those items. A re-export occurs when a covered item that has previously been exported out of the United States is again shipped or released to a third country. A transfer occurs when a controlled item previously exported to a

[15] 15 C.F.R. § 734, 22 C.F.R. § 120.
[16] 15 C.F.R. § 734.4.
[17] 15 C.F.R. § 734.3(a).
[18] 15 C.F.R. § 734.13; 22 C.F.R. § 120.17.

foreign country is provided to a different user or applied to a different end-use within that same country. In this regard, U.S. export controls typically follow the items they cover, even restricting transactions that occur entirely outside of the United States and that involve only non-U.S. persons.

Both regimes also generally restrict to whom covered items may be exported, re-exported, or transferred. The ITAR's restriction is quite broad: the provision of all covered defence articles and defence services to any foreign person must either be authorized or exempt from the need for authorisation.[19] The EAR only controls the provision of certain covered items to certain destinations or end-users or for certain end-uses. Different restrictions may apply to the export of an EAR-controlled item depending on where it is to be shipped, who will use it, and how it will be used. The same item exported to France, to a Russian energy company, or for use by the Chinese military would likely be subject to different EAR-based controls in each case.

B. Tools for Regulating – Item-Based, End-User and End-Use Controls

The U.S. Department of State (in the case of the ITAR) and the U.S. Department of Commerce (in the case of the EAR) implement these export controls through an item-based classification system and end-use and end-user controls, related licenses, and enforcement actions.

1. Item-Based Controls

Under both legal regimes, item-based controls are premised on classification systems that provide detailed descriptions of physical characteristics and performance parameters of the items subject to the controls. In order to evaluate what controls apply to an item for export, prospective exporters of U.S.-origin items must first determine which list—either the ITAR's United States Munitions List ("USML") or the EAR's Commerce Control List ("CCL")—includes a description of their item (i.e., the item's export controls jurisdiction) and then match their item to a description on the appropriate list to determine the item's classification (on the CCL, an item's classification is rendered as an alphanumeric sequence called the Export Controls Classification Number, or "ECCN"). The item's classification—taken together with its proposed destination, end-user, and end-use—determine which controls apply. On the CCL, different classifications of items are controlled for differing reasons (e.g., concerns about chemical weapons

[19] 22 C.F.R. § 123.1.

proliferation, human rights abuses, or crime control) and to differing extents. Depending on the applicable reasons for control and an item's destination, some exports may be effectively prohibited while others may be exported without further action.

These restrictions not only implement U.S. foreign policy but also often result from multilateral arrangements to impose similar controls among trading partners, including the Wassenaar Arrangement. This coordination helps to ensure a more equitable trading landscape among partner nations, but also slows the process for implementing new controls. Controls can always be imposed unilaterally in response to the United States' particular foreign policy concerns, but the U.S. is sensitive to the overreliance on unilateral controls as they may drive business away from the United States.

Requiring prior government authorisation is the primary means for controlling the export, re-export, or transfer of covered items. Like the CCL, the USML implements both U.S. foreign policy and national security policies as well as multilateral arrangements and treaty obligations in its item-based controls. In contrast to the CCL, however, exports of all items on the ITAR's USML are controlled in the same way. Exporters must obtain authorisation from the U.S. Department of State—whether in the form of a license or approved agreement—before exporting any item listed on the USML to any foreign person, unless one of several exemptions applies. Licensing policies established in the ITAR or by the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC"), which administers the ITAR, determine how requests for authorisation will be considered and, consequently, the relative strength of the ITAR controls. For example, the State Department will deny requests for authorisation to export ITAR-controlled defence articles to China, though requests for authorisation to export those same items to a different country may be reviewed and approved on a case-by-case basis. In addition to controlling exports with authorisation requirements, the ITAR requires that manufacturers, exporters, and brokers of covered defence articles and defence services register annually with the State Department and notify the agency of any changes to their ownership, location, or other identifying information.[20]

The EAR also relies primarily on license requirements and related licensing policies to control exports of subject items. However, unlike the ITAR,

[20] 22 C.F.R. § 122.1.

authorisation requirements under the EAR may vary based on an item's destination (as well as its end-user and end-use, as described further below). An item requiring a license for export to China may not generally require a license for export to France. Also, unlike the ITAR, the EAR does not require a license for exports of all covered items—or even for all items included on the CCL. However, like the ITAR, the EAR does use a system of licensing policies, in addition to its license requirements, that also determine the strength of the EAR's controls. In this regard, not all licensing requirements are created equal.

2. End-User Controls

The U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), which administers the EAR, also employs several different types of end-user controls. These tools, which may be used to limit exports to broad categories of end-users or specific individuals or entities, are among the most powerful of these tools in BIS's arsenal. They are often implemented by designating the targeted end-user to one of several lists of prohibited parties, including, for example, the EAR's Denied Persons and Entity Lists—which include targeted end-users in at least 19 NATO Member States. Such end-user controls can be implemented unilaterally (i.e., without international coordination), independently (i.e., without further Congressional action), and relatively quickly.

Individuals or entities subjected to these restrictions may be designated to BIS's Entity List or Denied Persons List. Persons added to the Entity List are subject to additional licensing requirements and specific, often restrictive, licensing policies.[21] In some cases, this may effectively cut the designee off from U.S.-origin exports. Although the Entity List began as a way to restrict exports to entities known to divert items to weapons of mass destruction programs, it has since expanded to include entities that pose any number of risks.

Designation to the Denied Persons List results in even more severe restrictions. Denied persons may not apply for or use a license or license exception. They are also broadly prohibited from negotiations concerning, ordering, buying, receiving, servicing, or disposing of EAR-controlled items.[22] BIS may add a company to the Denied Persons List as a penalty for violating the EAR or as a protective restriction. As the recent actions against ZTE and

[21] 15 C.F.R. § 744.16.

[22] 15 C.F.R. Supplement No. 1 to Part 764.

Huawei illustrate, these tools can have a significant, negative impact, especially when imposed on entities operating in industries that are heavily dependent on U.S.-origin parts and components.

3. End-Use Controls

End-use controls prevent items from being exported for, *inter alia*, use in certain nuclear applications, for chemical and biological weapons proliferation, and in certain nations' military activities—potentially imposing license requirements on cooperative development by NATO Member States of certain weapons technologies. These controls are the least frequently deployed of the controls listed here, in part because concerns about an item's end use are also often indirectly addressed by end-user or destination-based controls. The difficulty of complying with these restrictions may also discourage their imposition. While the prohibited end-uses are described in the regulations, it can be difficult to discern how a customer intends to use an item. Exporters must rely on additional due diligence review, contractual protections, and in some cases, specific certifications that the item will not be applied to prohibited end-uses. However, there may be little recourse if these prohibitions are violated by customers.

Compliance with all the various types of export controls—including end-user, end-use, and destination-based controls—is predicated on a technical evaluation of a product's performance characteristics and careful comparison to the USML and CCL. From that standpoint, compliance with item-based and end-user controls is relatively straightforward. The positive lists of controlled destinations and targeted persons make clear which exports are subject to the relevant restrictions. Exporters often know the locations and parties to which they are sending their products and therefore typically have access to the information necessary to confirm compliance. Furthermore, because end-user controls are an essential feature of U.S. trade controls—both export controls and sanctions—screening for prohibited end-users is a regular part of most well-developed trade compliance systems and there are a variety of tools readily available to assist companies in maintaining compliance with these restrictions. However, as with end-use controls, exporters may also wish to conduct additional due diligence to confirm that the recipient of their products does not plan to re-export the products to a prohibited destination or end-user.

Importantly, the licensing policies for each type of control described above—including item-based, end-user, and end-use controls—have been

calibrated to facilitate trade and interoperability among allies, in keeping with the U.S. export control regime's foundation in multilateralism and concerns about military preparedness. Both the ITAR and EAR generally control exports to allies—including NATO Member States—more permissively. In addition, both regimes include license exceptions and exemptions that specifically facilitate NATO-related trade, including special ITAR exemptions for trade with Australia, Canada, and the United Kingdom, which were implemented pursuant to different bilateral agreements with those nations.[23]

II. Recent Developments: Export Control Reform Act and Recent Changes to U.S. Law

With that general understanding of U.S. export controls in mind, it is important for members of the NATO community to understand how U.S. export controls have recently changed and will soon evolve.

The John S. McCain National Defense Authorization Act for Fiscal Year 2019,[24] which became law on August 13, 2018, contained two pieces of legislation that will have a significant impact on investment and technology transfers in the U.S. defence sector for decades to come. First, the bill contained the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"),[25] which significantly expands the scope of inbound foreign investments subject to review by CFIUS. Second, the bill also included the Export Control Reform Act of 2018 ("ECRA"),[26] which gives the President, acting through the U.S. Secretary of Commerce, a mandate and new authorities to restrict the outbound transfer of "emerging and foundational technologies" and requires the Secretary of Commerce to include the health of the U.S. national defence industrial base as a factor when evaluating export control license applications. Both measures are likely to have significant effects on the NATO community going forward by, among other things, re-routing investment flows and restricting cross-border collaboration in defence-related technologies. In other words, depending on the strength of the controls and the technologies to which they apply, the human and financial capital necessary to develop these critical technologies—rather than flowing easily across borders—may become concentrated in particular

[23] *See e.g.*, 15 C.F.R. § 740.11; 22 C.F.R. §§ 123.15, 126.5, and 126.14-.17.

[24] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, 132 Stat. 1636 (2018).

[25] Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, §§ 1701-28, 132 Stat. 2174.

[26] Export Control Reform Act of 2018, Pub. L. No. 115-232, §§ 1741-81, 132 Stat. 2208.

allied (or adversary) states.

Recent changes to U.S. foreign investment restrictions and export controls have been driven by concerns about sensitive U.S.-origin technology falling into the wrong hands, including especially companies owned or subject to control by the Chinese state. Part of the impetus behind FIRRMA were studies which showed how non-U.S. companies, and especially Chinese firms, have been participating in a range of venture capital investments in early-stage, innovative technology companies.[27] The U.S. Congress was particularly concerned that China was using national investment policies and private sector commercial arrangements to force U.S. companies to provide their Chinese counterparts with access to basic and advanced technologies that would enable China to leapfrog decades of technological development and pose an even larger economic and strategic threat to the United States and its allies. Indeed, these policies and arrangements, such as technology transfer for market access arrangements, have been critical to the development of China's defence sector.[28]

Congress also heard from observers who sounded an alarm noting that, over time, certain foreign investors have modified their investment strategies in emerging technologies to include venture capital and green field investments,[29] which CFIUS lacked jurisdiction to review and block. The realisation that foreign technology transfers involving critical technologies were being insufficiently monitored and regulated prompted Congress to give the U.S. Government new authorities under ECRA to control outbound flows of technology.

To help regulate these transfers, ECRA requires the President to establish, in coordination with the U.S. Secretaries of Commerce, Defense, Energy and State, a "regular, ongoing interagency process to identify emerging and foundational technologies" that are essential to national

[27] *See, e.g.*, MICHAEL BROWN & PAVNEET SINGH, CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION (Defense Innovation Unit Experimental, Jan. 2018).

[28] *Id.*; Bradley Perrett & Michael Bruno, *Changing the Rules*, AVIATION WEEK, Vol. 180, No. 21, at 52-54 (Sept. 2018); OFFICE OF U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 (Mar. 22, 2018).

[29] "A green field investment is a type of foreign direct investment (FDI) where a parent company creates a subsidiary in a different country, building its operations from the ground up." James Chen, 'Green Field Investment' (INVESTOPEDIA, May 31, 2019).

security but not yet captured by any other critical technology list.[30] As these emerging and foundational technologies are identified, the Secretary of Commerce is to establish controls on the export, re-export, or in-country transfer of such technology, including requirements for licenses or other authorisations.[31]

ECRA does not offer a precise definition of the "emerging technologies" or the "foundational technologies" to be controlled by BIS. Instead, it offers criteria for BIS to consider when determining what technologies will fall within this area of BIS control.[32] BIS is then responsible for developing implementing regulations.

To begin the process of identifying emerging and foundational technologies, BIS issued an Advance Notice of Proposed Rule Making ("ANPRM") in November 2018, seeking public comments on how to identify emerging technologies.[33] BIS will also consider the development of emerging technologies abroad, the effect of unilateral export restrictions on U.S. technological development and the ability of export controls to limit the spread of these emerging technologies in foreign countries.[34]

BIS broadly describes emerging technologies as those technologies "essential to the national security of the United States" that are not already subject to export controls under the EAR or ITAR.[35] The ANPRM suggests that technologies will be considered "essential to the national security of the United States" if they "have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could

[30]Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(a)(1), 132 Stat. 2208, 2218. For example, FIRRMA expands the scope of transactions subject to CFIUS review to include not only transactions resulting in the ownership or control of U.S. businesses by foreign persons (as has traditionally been the case), but also *non-controlling* investments in any U.S. business that produces, designs, tests, manufactures, fabricates or develops one or more "critical technologies." For CFIUS purposes, the term "critical technologies" includes: the defense articles and services described on the International Traffic in Arms Regulations ("ITAR") United States Munitions List ("USML"); certain technologies identified on the Export Administration Regulations ("EAR") Commerce Control List ("CCL"); nuclear facilities and equipment identified in 10 C.F.R. Part 110; and select agents and toxins. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1703(a)(6)(A), 132 Stat. 2174, 2182.

[31]Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(b), 132 Stat. 2208, 2219.

[32]*See* Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(a)-(b), 132 Stat. 2208, 2218-21.

[33]Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (advance notice of proposed rulemaking Nov. 19, 2018) [hereinafter ANPRM].

[34]ANPRM at 58,201. Given the express limitations provided in ECRA, technologies produced outside the United States are unlikely to be targeted by the new controls, as unilateral U.S. export controls would do little to restrict the flow of these technologies.

[35]ANPRM at 58,201.

provide the United States with a qualitative military or intelligence advantage."[36] Although the ANPRM does not provide concrete examples of "emerging technologies," BIS provided a list of fourteen broad areas of technology[37] it viewed as subject to limited controls that could potentially be considered "emerging" and therefore subject to new, broader controls under ECRA once specific technologies are identified.

Meanwhile, the process for developing controls on "foundational technologies" will operate along a separate, but parallel, track.[38] While BIS has not yet issued a second ANPRM that identifies possible candidates for "foundational technology" controls, the agency is widely expected to do so in the coming months.

Once BIS has arrived at a definition for "emerging technologies" and "foundational technologies," respectively, along with a set of potential controls for each, BIS will likely publish a proposed rule (or rules) providing this information for a period of public comment. Those comments will undergo a process of interagency review, and BIS should then announce its final rule (or rules) providing the new controls on the export of emerging and foundational technologies.

Once specific emerging and foundational technologies are identified in the final rule(s), companies can expect that their proposed exports of these technologies will be subject to greater scrutiny, and at least for some countries, subject to a licensing policy of denial. This is because ECRA also obligates the U.S. Department of Commerce to gather and consider the kinds of information on foreign ownership that would normally be included in CFIUS submissions prior to its grant of an export license for emerging and foundational technologies. For example, if a proposed export transaction involves a joint venture, joint development agreement, or similar collaborative arrangement involving emerging and foundational technologies, the Department of Commerce is to "require the applicant to identify, in addition to any foreign person participating in the arrangement, any foreign person

[36]ANPRM at 58,201.

[37]These broad areas include: (1) Biotechnology; (2) Artificial intelligence and machine learning technology; (3) Position, navigation and timing technology; (4) Microprocessor technology; (5) Advanced computing technology; (6) Data analytics technology; (7) Quantum information and sensing technology; (8) Logistics technology; (9) Additive manufacturing (e.g., 3D printing); (10) Robotics; (11) Brain-computer interfaces; (12) Hypersonics; (13) Advanced materials; and (14) Advanced surveillance technologies. ANPRM at 58,202.

[38]*See* ANPRM at 58,202 ("Commerce will issue a separate ANPRM regarding identification of foundational technologies that may be important to U.S. national security").

with significant ownership interest in a foreign person participating in the arrangement."[39]

While it is unclear how the Department of Commerce will specifically implement these new policy and licensing directives, we predict that many companies seeking to export emerging and foundational technologies will find it more difficult going forward. Not only will they be required to provide more information regarding their proposed counterparties in their export license applications, such as information on their counterparties' ultimate ownership and their role in the U.S. defence industrial base, but the Department of Commerce will likely deny applications when key strategic competitors of the United States, such as China, are involved.

Moreover, any technologies that BIS identifies as emerging or foundational through this rulemaking process will be considered "critical technologies" for the purposes of determining CFIUS jurisdiction.[40] FIRRMA now requires that certain foreign investments in U.S. companies that deal in these critical technologies receive CFIUS review and approval. Under CFIUS's new regulations implementing FIRRMA, CFIUS must receive advance notice of certain types of non-controlling foreign investments in U.S. companies that design, test, manufacture, fabricate or develop critical technologies—including emerging and foundational technologies identified by BIS—for use in one of several listed industries.[41] In this regard, BIS's final determination regarding what constitutes "emerging and foundational technologies" will also impact the scope of CFIUS's expanded jurisdiction.

III. Factors Affecting the Impact of Export Controls on Emerging Technologies

The impact of new export controls on the further development of emerging technologies identified for new export and foreign investment controls, even among NATO Member States, is likely to vary based on several different attributes.

A. Relative Cost and Likelihood of Expected Payoff of Developmental Research

[39] Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(b)(3)(C), 132 Stat. 2208, 2220.
[40] Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1703(a)(6)(A)(vi), 132 Stat. 2174, 2182.
[41] 31 C.F.R. § 801.101 (2020).

Who may be willing to sponsor development research depends on the potential payoff relative to the investment. High-cost, risky investment in emerging technologies—made more expensive and riskier by the imposition of new export controls—may limit the number of entities willing and able to undertake research and development of these new critical technologies. In general, one would expect riskier, higher cost investments in developmental research to be pursued only by the best-resourced entities that can afford potential failure. In contrast, when there is a greater likelihood of returns on lower cost investments, more may be willing to make the initial investment required to bring products to market.

B. Cultures of Innovation

The relative impact of export controls on an emerging technology will also hinge in part on the cultural practices of technologists in the fields required to develop the technology, which may vary—even among close allies. For a range of reasons, technologists in a particular field may already share freely and frequently as innovations occur. Technologists in other fields, for example, in fields where more investment is required to generate new products, may be less inclined to share particular innovations or the results of attempts to apply them beyond the walls of their respective employers.

When a specific field of emerging technology has a more open culture of innovation, export controls that seek to channel innovation may be more disruptive and may be less effective in channelling further innovation when compared with fields with more closed innovation cultures.

C. Emerging Technology-Specific Drivers for Collaborative Innovation

Alongside the economics and cultures of innovation in particular fields of emerging technology, there may be inherent drivers in some fields that lead technologists to collaborate. Generally speaking, if there is an expectation that a particular emerging technology may lead to development of products that will be more ubiquitous in people's lives, technologists may work to throw open the development of security standards and functions for these technologies to ensure that their applications are better vetted and trusted by others. In contrast, if emerging technology products are more likely to be adopted by only a few actors and in limited applications, technologists are more likely to keep the development of security for their products proprietary. For example, researchers in both

quantum computing and AI may have strong public policy interests to collaborate with one another in the development of common security protocols.

Given the potential power of quantum computing to breach the encryption algorithms used to secure so many aspects of modern-day communications, finance, and privacy, researchers have strong incentives to collaborate with one another on the development of quantum-safe cryptography. Similarly, given the potential ubiquity of AI-enabled applications in people's everyday lives, researchers have strong public policy incentives to ensure that AI-enabled applications cannot be hacked.

Other related drivers are the potential for an emerging technology to become a platform technology—i.e., the basis upon which other technologies or applications are developed—or the need of emerging technology applications to share platforms with others. Technologists may have strong incentives to be the first movers in particular areas of technology and to open their technology to others that will use it to develop applications based on their technology and draw still others to the new platform. Similarly, when a technologist knows that they will, by necessity, need to share infrastructure with other competitors, they may be more inclined to participate in the development of common standards and functionality.

D. Existing Export Controls on Emerging Technologies and Associated Technologies

The impact of new export controls on the development and proliferation of technologies is also likely to vary depending on whether there are already existing controls on associated technologies. Not all fields of emerging technology draw from fields of research that are already subject to export controls. To the extent that they are, technologists are already subject to limits on the dissemination of development technology through pre-publication review and licensing and the impact of new export controls is more likely to be only incremental.

E. Pre-Existing Distribution of Innovation

Whether and how controls could impact the development and proliferation of an emerging technology are also dependent on the underlying distribution of research in the relevant fields. If researchers in only a single country or a small set of countries are currently pursuing research in a particular subject area, ring fencing around the perimeter of this innovation

could potentially be effective in limiting its further proliferation. In contrast, such controls may be less effective at controlling a technology's proliferation, or proliferation to specific actors, if there are many more centers of innovation. When innovation is multi-centered, however, export controls could lead to a reduction in cross-fertilisation of technological ideas and abet the development of multiple advanced but divergent forms of the technology.

F. Managed vs. Unmanaged Innovation

The impact of export controls on the development of an emerging technology will also hinge in part on whether subsequent innovation is being centrally managed. Although a government may invest in the fundamental research required to lay the groundwork for an emerging technology, how export controls may impact the development of the technology may depend in part on whether the investment that follows is managed or unmanaged. For example, if export controls cut off a particular country and its researchers from a required building block for product development, a centrally managed system is more likely to be able to channel investment to the development of replacements. While those pursuing innovation in less centrally managed systems may also be able to identify a gap and channel research to fill it, they may not be able to do so as quickly or as effectively.

IV. Likely Impacts of New Export Controls on Two Types of Emerging Technologies

Finally, for a glimpse into how the forthcoming U.S. export controls on emerging technologies may play out in the real world, we offer two case studies. By applying the factors described in the previous section to a pair of technologies likely to be crucial to NATO's future military capabilities—hypersonics and artificial intelligence—it is possible to see how U.S. export controls, depending on how they are written, may cause innovation to become concentrated behind national borders.

A. Hypersonics

The term "hypersonics" describes technologies that enable aircraft, missiles, and other projectiles to travel at speeds of over Mach 5, or five times the speed of sound.[42] The technology has potential civil applications if it can

[42] *See, e.g.*, Congressional Research Service, 'Hypersonic Weapons: Background and Issues for Congress' R45811, (Mar. 17, 2020) 2.

be deployed in a manner safe enough to power commercial aircraft, but the primary application of hypersonics is military. For example, Russia claims to have now developed, tested, and deployed missiles that can travel as fast as Mach 27 and, if this claim is true, there is no defence system currently deployed anywhere in the world that would be able to intercept. Moreover, given the speed at which they would travel, hypersonic attacks would be more difficult to detect and would provide those targeted only a short period of time to respond.[43]

Fundamental research on hypersonics is occurring in multiple sites around the world, including China, the United States, Germany, France, Australia, and Russia, among other countries. According to a presentation count at the AIAA International Space Planes and Hypersonic Systems and Technologies Conference, China-based researchers have been the most prolific.[44] In contrast to China, which is managing a more integrated university research effort by placing large numbers of researchers focused on hypersonics in the same location, university research in the United States has been decentralized and less coordinated to date.[45]

Table 1: Top Ten Countries Presenting Papers at AIAA International Space Planes and Hypersonic Systems and Technologies Conference (2005-2017)[46]

Country	2005	2006	2008*	2009	2011	2012	2014	2015	2017	Total
China	7	17	4	15	18	31	3	42	260	397
U.S.	61	64	38	38	60	15	18	32	14	340
Germany	11	17	16	30	28	25	10	18	9	164
France	22	13	13	16	16	15	5	18	8	126
Australia	8	24	7	20	10	26	8	13	7	123
Japan	21	17	16	14	13	20	4	7	1	113
Italy	27	10	7	19	16	8	0	7	5	99
European groups[2]	6	6	6	8	9	5	1	8	6	55
Russia	14	5	6	4	3	6	0	5	5	48
U.K.	2	5	0	6	3	4	1	13	4	38
Total	**179**	**178**	**113**	**170**	**176**	**155**	**50**	**163**	**319**	**1,503**

Source: IDA Science and Technology Policy Institute
* International Space Planes and Hypersonics Systems and Technology Conference is not held every year.

[1] Other nations presenting papers at the 2017 conference were Algeria, Belgium, Brazil, Canada, Greece, Hungary, India, Iran, Netherlands, Norway, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan and Turkey.

[2] European organizations

[43] R. Jeffrey Smith, 'Hypersonic Missiles Are Unstoppable. And They're Starting a New Global Arms Race' *NY Times Magazine* (New York, June 19, 2019).
[44] K. Button, 'Hypersonics Weapons Race' *Aerospace America* (June 2018).
[45] *Id.*
[46] *Id.*

China, Russia, and the United States are on the shorter list of countries that have been able to move beyond fundamental research and into development, testing, and even deployment, in part because there are high barriers to entry in the further development of hypersonics and their associated technology. For example, hypersonic weapon testing in the United States relies in part on the prior existence of high velocity wind tunnels capable of simulating the wind speed and resistance that aircraft and projectiles traveling at higher than Mach 5 speeds would encounter. Moreover, the further development of hypersonic technology also requires innovation in several different fields, including ceramics, metallurgy, composite materials, and propulsion. Each of these associated technologies have their own high development costs and, as a result, tend to be pursued by larger private sector entities who are better able to afford research and development investment with more uncertain pay-offs.

The United States currently lags behind China and Russia in the development and field testing of hypersonic weapons and is now spending billions of dollars to catch up.[47] For example, the fiscal year 2019 U.S. Department of Defense budget included USD $2.6 billion for hypersonics development and the largest contract awarded went to Lockheed Martin to develop hypersonic missile systems for B-52 bombers and Air Force jets.[48] The fiscal year 2020 U.S. Department of Defense budget funded the creation of a university consortium to provide the Defense Department with increased access to foundational research, technology development, and workforce expertise. It also allocated over USD $500 million to support the rapid prototyping of hypersonics among other investments. Thus, while the United States currently lags both China and Russia in hypersonic development, it is investing significant sums now to catch up to and surpass its strategic competitors. Depending on how the United States opts to control the hypersonic technologies it is developing, NATO allies may or may not be involved in, or have opportunities to co-develop and use, hypersonic defensive and offensive weapons systems.

Although those conducting fundamental research into hypersonics are likely to continue publishing research papers, technologists working to develop and flight test hypersonic technology are less likely to freely share

[47] Anthony Capaccio, 'Pentagon to Test Hypersonic Missiles at Five Times the Speed of Sound' *Bloomberg* (Jan. 28, 2020).
[48] *Id.*

with others outside their particular sponsoring organizations. University researchers conducting applied projects are often subject to pre-publication review and clearance, and private sector engineers are typically precluded by their employment agreements from sharing their discoveries. Moreover, already-existing export controls, such as the ITAR, prohibit the public dissemination of technology associated with weapons systems without U.S. agency approval or licensing. Accordingly, even robust U.S. export controls on hypersonics are unlikely to alter the already closed and compartmentalized research landscape.

B. Artificial Intelligence

AI is not a single technology but a set of related technologies that aim to mimic different aspects of human intelligence. While the development of AI powerful enough to mimic general human intelligence is viewed by many as several decades away, there are a plethora of narrow AI applications that perform defined tasks such as strategic game play, natural language processing and translations, and image recognition. Narrow AI applications are typically developed using large data sets and specific algorithms to make increasingly robust predictions about the future.[49] The data used for machine learning can be either supervised (i.e., data that is already associated with other facts, such as labels) or unsupervised (i.e., raw data that requires the AI application to identify data patterns without prior prompting). This includes reinforcement learning—where machine-learning algorithms actively choose and even generate their own training data.[50]

Research into AI is global, with significant centers of innovation in the United States, Europe (particularly the United Kingdom and Germany), Japan, and China.[51] In the United States, AI is being pursued across universities, in the military, and throughout the private sector, with the most significant amount of money being spent in the commercial sector. A McKinsey Global Institute study estimates that the commercial sector invested between USD $20 to 30 billion in AI research in 2016 and estimates that this number will increase to USD $126 billion by 2025.[52] In contrast, U.S. Department of Defense unclassified

[49]Joshua Meltzer, 'The Impact of Artificial Intelligence on International Trade' *Brookings Institution* (Dec. 13, 2018).
[50]*Id.*
[51]Bruno Jacobson, 'Five Countries Leading the Way in AI' *Future Trends* (Jan. 8, 2018).
[52]McKinsey Global Institute, 'Artificial Intelligence, The Next Digital Frontier?' (June 2017) 4-6.

expenditures on AI totalled only USD $600 million in 2016.[53] Given the order of magnitude difference between commercial and military investment in AI technologies in the United States, some observers have suggested that the Defense Department partner with the private sector to further develop military applications. However, there is strong scepticism of such partnerships among commercial leaders in the field, making the management of further innovation in AI decentralized and uncoordinated. In contrast, AI innovation in China is reported to be more centralized and intentional, and few boundaries exist between Chinese companies, university research laboratories, the military, and the central government.[54] To the extent the Chinese government identifies promising fundamental or applied AI research, it has a more direct way to guide further development.

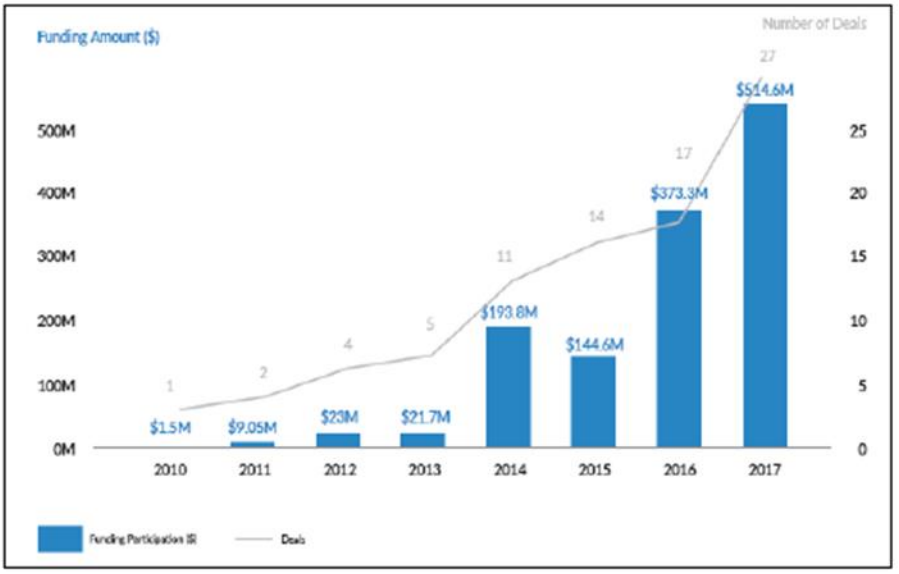
In contrast to other kinds of emerging technologies, AI has relatively low barriers to entry, at least with respect to AI software development. Although finding programmers with the requisite talent can be costly, many centers of AI research make training courses on AI available for free online and host environments, libraries, and data sets for those learning AI coding to train, program, and test AI applications. In addition to the relatively low level of investment required to learn AI programming, robust computing power and AI training software are also now available to customers through cloud-based services that can be rented from global providers like Microsoft Azure, Amazon Web Services, Google Cloud, and Alibaba Cloud.

In contrast to AI software development, there are higher barriers to entry to the design of AI-capable chips and their fabrication, barriers that largely replicate those that already exist for other areas of semiconductor manufacture, in which only a small number of companies compete to etch more and more computing power and efficiency onto smaller and smaller wafers. The life cycle for design, development, and production of new chips often spans several years, and there is only a small handful of companies in the United States, Taiwan, Japan, and South Korea that are capable of fabricating the most advanced semiconductors once designed.[55] Another key limit on AI development is the availability of bias-free, error-free and labelled data sets that readily can be used to train and test AI and machine

[53]Congressional Research Service, 'Artificial Intelligence and National Security' R45178, (Jan. 30, 2019) 6.
[54]Gregory C. Allen, 'Understanding China's AI Strategy' *Center for New American Security* (Feb. 6, 2019).
[55]*See generally*, Deloitte, 'Semiconductors – The Next Wave' (April 2019).

learning applications.[56]

Figure 2. Chinese Investment in U.S. AI Companies, 2010-2017



Source: Michael Brown and Pavneet Singh, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, Defense Innovation Unit Experimental, January 2018, https://www.diux.mil/download/datasets/1758/DIUx%20Study%20on%20China's%20Technology%20Transfer%20Strategy%20-%20Jan%202018.pdf, p. 29.

In contrast to those working in hypersonics and other emerging technologies, AI technologists freely share the results of their work in research publications and through a range of online platforms such as GitHub, arXive.org, and H2O.ai. Many of the algorithms used in AI today are publicly available, and university and even applied AI researchers working with these algorithms will often move to quickly publish their work both to demonstrate proof of concept for their implementation and also to help accelerate the review and vetting of innovations by peer technologists. Moreover, similar to making operating system source code freely available to encourage programmers to develop new applications, several of those providing AI services frameworks also make them open source to help accelerate the further development of new applications and the wider adoption of particular AI service provider platforms.[57]

Another key contrast with hypersonics research is the relative lack of

[56] *See e.g.*, 'Almost 80% of AI and ML Projects Have Stalled, Survey Says' *Robotics Business Review* (May 23, 2019).
[57] Patrick Shafto, 'Why Big Tech Companies are Open-Sourcing Their AI Systems' *The Conversation* (Feb. 22, 2016).

export controls on AI today. While there exist certain controls on software and semiconductor design and fabrication technology, with only one exception, U.S. export controls have not been framed around AI-enabled applications, and neither machine learning nor smarter kinds of AI are themselves objects of control under either the EAR, the ITAR, or international regimes such as the Wassenaar Arrangement. On January 6, 2020, the U.S. Department of Commerce imposed new controls on software that uses AI to automate the analysis of geospatial imagery and point cloud data.[58] As a result, when new, application-specific AI controls are imposed, many researchers in AI will experience new and significant impacts on their ability to freely share and collaborate on that specific application and any iterations that rely or build on it.

C. Probable Impacts of New Export Controls on Technology Development and Interoperability

Given the foregoing development characteristics of hypersonics and AI, we can make reasonable predictions of how different types of U.S. export controls are likely to be applied and how they are likely to impact both U.S. and international technological development in each field.

1. Impact of New Emerging Technology Controls on Hypersonic Development

First, because many of the fields required to advance hypersonics are already subject to multilateral export controls, the applied research communities working in the United States on hypersonics will likely be able to continue cross-border collaborations in much the same way as they have performed to date: under specific export licenses authorising only certain collaborations with counterparties outside of the United States. Second, because of the high barriers to entry, further development of hypersonics, especially hypersonic vehicles that integrate research and development from hypersonics' associated fields, will continue to be a limited pursuit of only large defence contractors, who are best placed to make and receive the kinds of investments necessary to further develop and apply advancements in the several different areas of fundamental research required for hypersonics. Third, further development of hypersonics is likely to result in divergent development with multiple, different proprietary designs being

[58] Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series, 85 Fed. Reg. 459 (Jan. 6, 2020).

pursued by researchers who have not engaged in the kind of open-source collaboration that has characterized development in fields like AI. Fourth, because only a few private sector entities and applied research centers will be in a position to develop hypersonic offensive and defensive capabilities, there will not be the same incentive to develop open and widely-shared security protocols to protect access to hypersonic technologies as there would be for technologies that are expected to be more widely adopted in civil applications. Taken together, these factors will likely act together to cluster hypersonics development into only a small number of companies and government-funded research institutes in the United States, Europe, Russia, and China, with each developing independently from one another unless national export authorities allow, and multilateral institutions like NATO and its membership sponsor the integration of research and development, application, and production. While the United States' new export controls on hypersonics and associated technologies will almost certainly restrict the flow of these technologies and resulting weapons systems to strategic competitors like Russia and China, the already existing NATO and NATO member investment in the development (including co-development) of hypersonics could provide the United States with an incentive to fashion controls that include NATO and NATO Member States in U.S. development efforts.

New deemed export licensing requirements, which hinge on item-based controls, are less likely to have a significant impact on hypersonics development because many U.S.-based defence contractors are already accustomed to the kinds of hiring and technology controls required to implement these restrictive measures, and have likely already obtained licensing for any non-U.S. person technologists working in the several areas of technology required to further develop and test hypersonics research.

U.S. and multilateral export controls on end-uses and end-users are also likely to intensify the clustered and divergent development of hypersonics. In addition to item-based U.S. export controls, the contributions that hypersonics can make to both ballistic and nuclear weapon proliferation also makes applied hypersonics potentially subject to end-use and end-user licensing requirements. These kinds of export controls have the effect of ensuring that only authorised persons and entities outside of the United States receive technology and other items controlled for these purposes, further reinforcing collaboration channels with specific end-users and also making it less likely that hypersonics technology will be shared with those considered to be adversaries of the United States. The recent expansion of CFIUS's jurisdiction to

review certain non-controlling, as well as controlling, investments in U.S. businesses is also unlikely to have a significant impact on the development of hypersonics. Given the sector's high barriers to entry and the substantial role played by large defence contractors in developing such technology, there are already limited avenues for foreign investors to acquire a significant interest in one of the handful of U.S. businesses capable of developing hypersonics. As FIRRMA is fully implemented, opportunities for non-U.S. persons to invest in such technology are likely to remain similarly constricted.

2. Impact of New Emerging Technology Controls on AI Development

Although the significant investments required to develop and fabricate new AI hardware will continue to limit the number of entities that can work on AI hardware, AI software has been and will continue to be widely distributed and pursued globally, wherever talent can be found. The relative lack of existing export controls on AI and the widespread practice of open sharing of innovation and collaborative work on common AI standards among software developers will make it difficult to impose new export controls that will not be significantly disruptive.

Item-based controls on AI, such as on AI software and technology applied to specific military and dual-use items, are likely to cause AI development to fragment in different ways. The United States would presumably impose item-based controls in ways that limit transfer of AI technology to strategic competitors such as China and Russia, but allow licensed transfers to strategic allies of the United States such as NATO members, plus Australia, Japan, New Zealand, Sweden, and South Korea, or some subset of these countries. However, given that China is already a leader in AI research, it is likely that these controls will cut off at least U.S. researchers from certain innovations occurring in China and in multinational collaborations that include China. This could lead to divergence between U.S. and Chinese AI innovations and could undermine efforts to develop global security standards for access to AI-controlled applications. While U.S. item-based controls on AI are likely to leave open the potential for continuing collaboration with U.S. allies in NATO and Asia, export licensing is likely, at least at the outset, to hinder many ongoing collaborations. Moreover, U.S. allies are likely to be subject to significant geopolitical pressure from countries on the outside of the U.S. export control ring fence, especially China, who will continue to develop AI applications that may rival and even surpass U.S.

technologies in specific applications. Individual NATO countries will therefore likely be placed in the difficult position of trying to choose between divergent U.S. and NATO-developed AI applications and Chinese ones, the latter of which are likely to be less costly.

New, item-based deemed export licensing requirements are likely to have significant, disruptive impacts on the development of AI technologies. U.S. AI start-ups and technology giants alike rely on large numbers of non-U.S. technologists, with some companies employing non-U.S. person technologists numbering in the many thousands. Because AI and AI applications have not historically been the subject of significant export controls, many technology companies have not yet developed the internal compliance architectures required to identify potential licensing requirements or to keep separate licensed and unlicensed technologists within their companies. Especially for AI researchers who, for reasons discussed above, are already strongly predisposed to collaboration, these AI start-ups and product development teams within larger technology companies are likely to be severely impacted by new controls. This disruption—including the potential that the U.S. Government will delay or deny licenses to support leading non-U.S. technologists in their work—may cause many of these highly specialized personnel to search for employment opportunities outside the United States.

To the extent more targeted end-use and end-user controls are applied to AI innovation,[59] such controls may be less disruptive to current patterns of innovation and may be less likely to lead to significant divergence across countries and innovation ecosystems. With end-use controls, only certain applications of AI would be targeted and export authorities would have the opportunity to review and channel technological exchange toward certain projects and research collaborations and away from others. Similarly, end-user controls would only prevent certain end users, such as the applied research institutes and other organizations of strategic competitors, from obtaining U.S. or NATO technology.

Moreover, the CFIUS review process is likely to significantly disrupt cross-border investments in AI technology. Currently, China and the United States are among the leading centers of AI innovation and are also the top destinations for venture capital investment in AI technologies—with Chinese AI companies raising USD $31.7 billion during the first half of 2018, out of a

[59] *See id.*

global total of USD $43.5 billion.[60] However, since the Trump administration came to office in 2017, Chinese foreign direct investment in the United States across all sectors has fallen by approximately 90 percent, driven in part by heightened CFIUS scrutiny of China-based deals.[61] Indeed, while China has historically been a significant source of inbound investment in the United States, most of the transactions that have been blocked by the Committee to date either involved a Chinese acquirer or were motivated by concerns regarding Chinese competitors. Although CFIUS continues to clear Chinese deals, CFIUS review may result in lengthy delays and the imposition of significant mitigation measures. Accordingly, the prospect that the U.S. Government may delay, condition, or reject Chinese investments in U.S.-based AI companies may further chill foreign investment in the sector and cause Chinese and other foreign investors to instead direct their investment dollars toward homegrown AI companies.

Conclusion

Since publishing its list of potential targets for the new emerging technology controls,[62] BIS has signalled that the new controls will be more narrowly tailored—perhaps focusing on specific applications of emerging technologies—rather than broad controls on all items falling within any of the categories listed in the ANPRM.[63] It is possible that the new controls may be structured similarly to the restrictions BIS imposed on AI-driven geospatial imagery software in January 2020, which used specific performance characteristics to target a specific application of AI.[64] Such narrow tailoring could help to limit the new controls' impact. However, BIS officials have also cautioned that there will likely be more than one round of new emerging technology controls, and restrictions on foundational technology are still forthcoming.[65] The combined effect of these new controls—or simply the anticipation of their impact—could restrict international collaboration and slow development of the targeted technologies.

---

[60] Xiaomin Mou, 'Artificial Intelligence: Investment Trends and Selected Industry Uses' *IFC Emerging Markets Compass* (Sept. 2019) 2, Note 71.
[61] *See, e.g.*, Alan Rappeport, 'Chinese Money in the U.S. Dries Up as Trade War Drags On' *NY Times* (New York, July 21, 2019).
[62] *See* ANPRM.
[63] Ian Cohen, 'Companies, Trade Groups Concerned over Emerging Tech Controls' *Export Compliance Daily* (Nov. 8, 2019) [hereinafter Cohen, *Companies, Trade Groups Concerned*].
[64] Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series, 85 Fed. Reg. 459 (Jan. 6, 2020).
[65] Cohen, *Companies, Trade Groups Concerned*.

As described above, the effect of these new controls will also depend on several factors endogenous to the targeted industries. New export controls are likely to have a less significant impact for industries where the existing barriers to entry are already high or where the research and development culture is less collaborative. Current practices for sharing technology, existing export controls, and established distributions of capacity will all affect the extent to which new export controls shape the development of emerging and foundational technologies.

The impact of these new controls also depends on how they are implemented—whether they remain unilateral controls or are also adopted by U.S. allies. There are early indications that the United States hopes to make these new restrictions multilateral. Not only does ECRA require coordination with multilateral export control regimes, but BIS officials have also indicated that they plan to present the new controls on emerging technologies for adoption by the members of the Wassenaar Arrangement through the group's regular decision-making process.[66]

The United States has recently shown an interest in taking a multilateral approach in other areas of U.S. trade controls, encouraging international alignment by offering a reduced regulatory burden to those who adopt its policies and processes. New CFIUS regulations provide favourable treatment for businesses from countries that adopt a similar structure for national security review of inbound foreign investment.[67] Meanwhile, BIS has proposed removing license exceptions for re-exports from Wassenaar countries to jurisdictions of national security concern because of concerns BIS has about the different license review standards that the United States and its allies apply to such exports.[68] The implication of the proposed rule is that a realignment of those review standards by U.S. allies could mean the current license exception stays in place.

By first taking unilateral action and then pursuing multilateral adoption, the United States is indicating that—while it would prefer not to "go it alone"—the national security risks presented by the current regulatory landscape are sufficiently great that a unilateral response is preferable to no

[66]Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(c), 132 Stat. 2208, 2221; Cohen, *Companies, Trade Groups Concerned*.

[67]*See* Provisions Pertaining to Certain Investment in the United States by Foreign Persons, 84 Fed. Reg. 50,174, 50,179 (Sept. 24, 2019) for an explanation of the new "excepted foreign state" status implemented in 31 C.F.R. §§ 800.218 and 800.1001.

[68]Modification of License Exception Additional Permissive Reexports (APR), 85 Fed. Reg. 23,496 (Apr. 28, 2020).

response at all.

In the short term, this control-now-cooperate-later approach could lead to a divergence in export controls that negatively affects the speed with which emerging technologies continue to develop and the interoperability of items made using these controls. If efforts to encourage international adoption of these restrictions fail, a fragmented regulatory environment could develop in the longer term—with separate controls adopted in the United States, EU, and China. Depending in part upon the factors described above, U.S. industry could suffer as revenue from restricted jurisdictions is lost and competitors gain market share. Development of important technologies could also move offshore in search of more favourable regulatory environments. Such shifts could also harm U.S. allies, as technical development slows or becomes inaccessible.

However, successful international coordination to control emerging and foundational technologies could expand the economic and security benefits of the current multilateral framework in the long term. Adoption of similar controls by U.S. allies in NATO would facilitate the development of those technologies and the interoperability of the cutting-edge items they will be necessary to produce. Just as Cold War collaboration on export controls helped to counter the threat of the Eastern Bloc and the Wassenaar Arrangement has helped to counter rogue states and international terrorism, multilateral adoption of controls on emerging and foundational technologies would help to ensure a coordinated approach by the United States and its NATO allies to address emerging threats to international security.

***

Source: https://www.innovationhub-act.org

The Relevance and Benefits of Integrated Compliance Strategy (ICS) for NATO Defence Forces

by Martijn Antzoulatos-Borgstein MSc. LL.M.[1]

Introduction.

This paper argues the NATO defence forces provided by the NATO nations should collectively innovate by employing an integrated compliance strategy to control military technologies, goods, software or data. With the emergence of new technologies[2] we have witnessed the international increase of alternative methods to put pressure on states, groups and organizations. Conflicts between states using their military forces as a method of exerting pressure[3] seem to have lost ground to less costly but very effective non-kinetic methods such as information operations[4] and cyber operations.[5] These cheaper methods are often used by non-state actors, acting independently or as a state proxy, outside the legal framework of armed conflict. Objectives can include sabotage of critical infrastructure, obtaining access to shielded industry and government data, oppression of local

[1] The author works for Rockwell Automation as Trade Compliance Manager for Europe, Middle East and Africa, and is a Reserve Officer for the Royal Netherlands Air Force. *The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO or ACT.*

[2] Such as: high automation, advanced robotics, man-machine interfaces, artificial intelligence, advanced information technology, big data analytics, 3D printing, bio-technologies.

[3] "The number of interstate conflicts continued to be low; the two conflicts recorded in 2018 were also active in 2019: Iran–Israel and India–Pakistan. "Therese Pettersson and Magnus Oberg. Organized violence, 1989–2019. Special Data Feature, Journal of Peace Research, 2020 p 2. Available at https://journals.sagepub.com/doi/pdf/10.1177/0022343320934986.

[4] Rand Corporation. Information Operations. 03-28-2020. www.rand.org/topics/information-operations.html

[5] S.W. Magnan. Are We Our Own Worst Enemy. Safeguarding Information Operations. Center for the Study of Intelligence, vol. 44, no. 3, 2019: pp. 97-103. Available at: www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no3/pdf/v44i3a08p.pdf (accessed: 03-28-2020).

populace, undermining of democratic institutions, influencing of financial markets, and even destabilization of economic power blocks.

The tools used vary from custom developed high-end government funded programs, to combinations of standard commercially available products, knowledge obtained from technical universities, social engineering techniques, and whatever is available on the internet. The targets chosen can range from electric powerplants, industries, social media platforms, election campaigns and stock-markets, to data servers of defence ministries. These emerging technologies and how they can be used for malign purposes, have revived the international interest in the use of trade controls, as a way of getting grip on proliferation and use of controlled technology. This grip focuses on both emerging technologies itself, and on the protection of critical goods or data that could cause harm when accessed by bad actors. Examples are: encryption and decryption source coding, engineering data on the functioning of critical weapon platforms and systems, genetic coding of biological agents that could be used as weapons, goods and data that could be used in the process to create nuclear weapons, or their delivery agents.

Trade controls are best understood as all laws and regulations that relate to economic, trade, and financial sanctions, as well as to the export, import, reexport, transfer and retransfer of tangible goods and intangible goods (i.e. controlled software or data). Goods, software or data subject to such controls can either be controlled for military reasons, or as goods, software and data with both a commercial and a potential military purpose (i.e. *dual-use*). The general idea behind these trade controls is to control imports (e.g. France, Israel, Poland, and Russia maintain entry notification, registration and licensing requirements for imports of goods and software containing certain grades of encryption) and to prevent or restrict access to sensitive technology (both controlled as military and dual-use) by countries, individuals or legal entities that are on international watch lists, maintained by states' intelligence agencies. Individuals or entities who deliver controlled technology to sanctioned parties, or to parties in countries that require an export license to be obtained, and who failed to comply with such requirements, risk penalties, loss of trade privileges, and even incarceration.

For most global operating companies or institutions that produce, sell or otherwise source, use and distribute controlled products and technologies all over the world, compliance with trade controls is second nature. This is

exemplified by high investments made in recruitment, development and retention of trade compliance officers, automation of enterprise resource programs, including trade compliance control processes, frequent internal and external auditing of processes, and training of their workforce. The combination of trade data collection and analysis, trade knowledge, internal control and monitoring processes that are used to comply with trade controls is called trade compliance. Trade compliance is usually overseen by trade compliance functions, responsible for execution of a trade compliance program.

Trade Compliance and NATO.

As a result of the above, trade compliance has become increasingly important for NATO nations whose military forces are users of various kinds of controlled goods and technology, and who are operating internationally and collectively. When national forces of NATO nations bring controlled goods and technologies across borders they are putting these controlled goods and technologies within reach of third-parties, including service suppliers and coalition partners, who may not always be eligible to receive or access such goods and technology.

This is especially important for those nations whose capabilities, companies, and national defence forces are subject to strictly enforced trade controls. Particularly, the domains of aerospace, automation, information technology, nuclear power, chemical production, bio-pharma, and weaponry are generally subject to strict trade rules and their enforcement. Significantly, the U.S. Government enforces its export control regulations (e.g. the International Traffic in Arms Regulations – ITAR, and the Export Administration Regulations – EAR), not only in the U.S. and against U.S. Persons,[6] but also against Foreign Persons,[7] inside and outside the U.S.[8] Traditionally, companies were the main subjects of attention, but focus has broadened to include international organisations, research facilities, governmental agencies, and their senior executives. This is exemplified by different prosecutions of individuals, including academic practitioners,[9] and

[6] International Traffic in Arms Regulations (ITAR), 22 C.F.R. §120.15.
[7] International Traffic in Arms Regulations (ITAR), 22 C.F.R. §120.16.
[8] M. Antzoulatos-Borgstein. Integrated Compliance Strategy. A research into the effects of business strategy on the compliance maturity level of aerospace and defence organizations. MSc thesis for the Executive Master in International Trade Compliance (EMITC) programme, London: University of Liverpool Management School, 2017, p.4.
[9] United States Court of Appeals, 6th Circuit. United States v. John Reece Roth, 628 F.3d 827, 6th Cir. 2011.

Foreign Persons[10] for wilful violations of the Arms Export Control Act or the International Emergency Economic Powers Act. Additional indicators are voluntary disclosures for trade control violations by foreign governments, and stricter U.S. Department of Justice policy with regard to the prosecution of organisations' senior executives.[11]

The necessity of increased scrutiny is emphasised by the many cases of espionage, economic espionage, and trade secret theft to which not only companies are subjected, but also not-for-profit organisations and individuals. This emerging threat was brought up again in 2017, by the Director of the Military Intelligence and Security Agency (MIVD) of the Kingdom of the Netherlands, who declared in the media that the Dutch secret services are suffering from a *substantial* number of attempts each year by foreign groups to acquire knowledge and materiel to manufacture weapons of mass destruction, and that organisations are not sufficiently aware of the risks they face in this context.[12]

Increased scrutiny calls for reinforced organizational risk management and effective trade compliance programs. Normally, such measures are covered by an organisation's Internal Compliance Programme (ICP), and governed by its trade compliance functions. However, whereas ICPs and trade compliance functions may be generally accepted and established instruments within business entities, these are not yet common within all NATO defence forces. This may indicate that, here, there is ground to gain for these NATO nations and their compliance officers.

Domains where trade compliance risks could be underestimated, are those of research and development, as well as maintenance and repair of

[10] United States Department of Justice. Summary of major enforcement, economic espionage, trade secret and embargo-related criminal cases. January 2009 to August 2015, NSD (202) 514-2007. Available at: https://www.pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf (accessed on: October 27, 2017).

[11] S.Q. Yates. Individual Accountability for Corporate Wrongdoing. United States Department of Justice, Office of the Deputy Attorney General, Memorandum, September 9. Available at: https://www.justice.gov/archives/dag/file/769036/download (accessed on: March 28, 2020).

[12] Dutch technology may have been used in weapons of mass destruction: ministers. Dutch News.nl. 10-26-2017. Available at: https://www.dutchnews.nl/news/archives/2017/10/dutch-technology-may-have-been-used-in-weapons-of-mass-destruction-ministers/ (accessed: March 28, 2020); B. Weinthal. Report: Dutch technology may have helped advance Iran's weapons program. Intelligence services from the Netherlands are raising a red flag over Iran's use of Dutch technology to accelerate its lethal weapons program. The Jerusalem Post, 11-04-2017. Available at: http://www.jpost.com/Middle-East/Iran-News/Report-Dutch-technology-may-have-helped-advance-Irans-weapons-program-513317 (accessed: March 28, 2020).

military platforms (e.g. fighter jets, submarines, command and control centres), their systems and components, or even the transportation of these. Since outsourcing of most of these activities has become a preferred method of managing material readiness at lower cost, the risks regarding unauthorised access, re-exports, re-transfers or releases of export controlled articles, technical data and defence services to third parties (e.g. commercial maintenance facilities, non-governmental scientific research facilities), espionage, theft of intellectual property, proliferation of sensitive technology, and threats to national and international security have increased.[13] A relevant but sometimes underestimated risk category is connected to the transfer of export controlled technical data over an unsecure and unencrypted datalink (e.g. normal internet) through third party providers and storage or retrieval through third party cloud environments. An internal compliance programme and a well-organized trade compliance department are key assets to assess, control and monitor these threats effectively and efficiently.

Relevance and benefits of an Integrated Compliance Strategy.

In the previous paragraph, the relevance of risk management and compliance tools, to assess and control trade compliance risks, was discussed. However, research shows that the level of effectiveness of such tools depends, for a large part, on the underlying strategy chosen. Especially for organizations that operate internationally, in a highly-regulated environment – such as aerospace & defence companies, and defence forces – only a well-balanced integrated compliance strategy (ICS) can significantly reduce the risk of material non-compliances.[14]

An ICS can be defined as a "Type of business strategy that not only supposes alignment of the elements of the 7-S Model to achieve financial performance (FP) objectives, but that integrates FP objectives and Ethics & Compliance (E&C) objectives (e.g. standards for responsible corporate conduct and other hard-to-measure objectives) into an amalgamated

[13] Antzoulatos-Borgstein, 2017, p. 27; D.B. Nast. Joint Ventures: Risks and Rewards, 2017. Available at: https://www.huffingtonpost.com/david-b-nast/joint-ventures-risks-and-_b_10803424.html (accessed: March 28, 2020);M. Erbschloe. International Technology Transfer. Research Starters: Business, 2015. Available at: http://eds.b.ebscohost.com.liverpool.idm.oclc.org/eds/detail/detail?vid=5&sid=bbe7565d-ce71-44a4-b111bee9660cb42e%40sessionmgr102&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2I0ZQ%3d%3d#AN=89163793&db=ers (accessed: March 28, 2020).

[14] Antzoulatos-Borgstein, 2017, pp. 20-22.

whole."[15]

This definition reveals that the basis for an ICS is the 7-S Model.[16] This is a dynamic strategy model that was developed by the American consultancy firm McKinsey in the 1980's, and still is widely used to date. The model is characterised by its organisation of hard elements--strategy, structure and systems—called 3-S and soft elements—staff, skills, style and shared values—called 4-S, that should all be aligned and operating in tune, to create a balanced outcome. The simplicity of the model and its focus on coordination rather than structure – which is ideally applicable in agile, rapidly changing environments – adds to its usability and popularity.[17]

Despite the success of the 7-S Model, alignment of hard and soft elements alone, does not lead to integration of financial performance objectives (which in the context of the defence forces of NATO nations, may be regarded as military capability objectives) and ethics and compliance objectives. In this context, an ICS aims to fill that gap. First of all, 3-S (hard element alignment) is distinguished from 4-S (soft element alignment) because 3-S is conditional for financial performance and military capability and 4-S is conditional for founding an ethical culture. However, both 3-S and 4-S are regarded as equally important. The presence and quality of an ethical culture is required for integration of ethics and compliance objectives. Research indicates that organisations that had successfully integrated performance objectives and ethics and compliance objectives, displayed both better performance figures and higher levels of compliance maturity.[18]

The model used to indicate organisations' compliance maturity is the capability maturity model (CMM), tailored for use in a compliance context. It consists of 5 levels, with each subsequent level indicating progression of an organisation's compliance maturity reflected by its ability to prevent or

[15] Antzoulatos-Borgstein, 2017, p. 83.
[16] "Our claim is that effective organizational change is really the relationship between structure, strategy, systems, style, skills, staff, and something we call superordinate goals. (The alliteration is intentional: it serves as an aid to memory.) "Robert H. Waterman, Jr., Thomas J. Peters, and Julian R. Phillips. Business Horizons, June, 1980: p.17. Available at: https://tompeters.com/docs/Structure_Is_Not_Organization.pdf.
[17] Antzoulatos-Borgstein, 2017, pp. 11-12; L. Bryan. Enduring Ideas: The 7-S Framework'. McKinsey Quarterly. 03-2008. Available at: http://mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/enduring-ideas-the-7-s-framework (accessed: March 28, 2020); R.S. Kaplan. How the balanced scorecard complements the McKinsey 7-S model. Strategy & Leadership, 13(3), 2005: p. 41; M.E. Porter. Towards a Dynamic Theory of Strategy. Strategic Management Journal, Vol. 12, Special Issue: Fundamental Research Issues in Strategy and Economics, 1991: pp. 95-117.
[18] Antzoulatos-Borgstein, 2017, pp. 42-46.

mitigate risk. The highest compliance maturity level (CML 5) equals residual risk—which is the amount of risk that remains after the compliance controls are applied.[19]

Both the CMM, and its modernised variant—capability maturity model integration (CMM-I)—have their roots in research conducted by NASA and the U.S. Air Force in the 1950's-1960's. This research focused on quality management improvement of software developed for and used in the context of civil and military space and missile programmes. The model aims to improve software development processes through a 5-level process maturity continuum. The Software Engineering Institute of the Carnegie Mellon University[20] was, and still is, the managing agency for CMM/CMM-I.[21] Although, CMM/CMM-I originated within the governmental sector, it is widely used today by companies all over the world. [22]

An ICS provides organisations the means to achieve CML 4 and 5 which means decreasing their exposure to material non-compliances to low (CML 4) and, respectively, residual (CML 5). It was established that the better the integration of both financial performance and military capability objectives and ethics and compliance objectives is, the higher an organisation's compliance maturity level can be.[23]

Benefits of an ICS are, first and foremost, insight and awareness of the risks related to the alignment and integration of financial performance (or military capability for NATO nations) and ethics and compliance objectives. For instance, in organisations where such awareness is absent or minimal, the risk of overemphasizing on strategy, structure, and systems (3-S) is present, which may lead to a one-sided approach to compliance,[24] that provides the

[19] Rachel Slabotsky. Inherent Risk vs. Residual Risk Explained In 90 Seconds. FAIR Institute Blog: September 7, 2017. Available at: https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds.
[20] Carnegie Mellon University, Software and Engineering Institute: https://www.sei.cmu.edu/.
[21] S. Kemp. The History and Purpose of the Capability Maturity Model (CMM). Tough Nickel, Business-Management, 05-12-2016. Available at: https://toughnickel.com/business/The-History-and-Purpose-of-the-Capability-Maturity-Model-CMM (accessed: March 28, 2020).
[22] C.J. Torrecilla-Salinas, et al. Agile, Web Engineering and Capability Maturity Model Integration: A systematic literature review. Information and Software Technology, Vol. 71, Issue C, 2016: pp. 92-107. Available at: https://www.sciencedirect.com/search?qs=torrecillas&authors=&pub=Information%20and%20Software%20Technology&volume=&issue=&page=&origin=journal&zone=qSearch&publicationTitles=271539&withinJournalBook=true (accessed: March 29, 2020).
[23] Antzoulatos-Borgstein, 2017, pp. 16-18
[24] M. Berzins and F. Sofo. The inability of compliance strategies to prevent collusive conduct. Corporate Governance, 8(5), 2008: pp. 669-680.

organisation with a false sense of security. The recent Volkswagen and Wells Fargo fraud cases indicate that a performance metrics-dominant approach can lead to blind-spots with regard to human behavioural risks such as unethical, deceptive or collusive conduct.[25]

Another benefit of an ICS is that it serves as a comprehensive strategic compass for senior management, taking into account, and integrating all relevant objectives, not only financial performance and military capability objectives and performance metrics. As such, an ICS can contribute to improve the quality of organisational decision-making, and to reinforce an ethical culture.

An ICS supports the functioning of an organization's internal compliance programme (ICP) and compliance functions, through its strategic alignment and integration of objectives. Since strategy lies at the basis of all other organisational activities, an ICS can catalyse the merger of the 4-S elements: staff, skills, style and shared values into the fabric of organisational culture and conduct, thereby facilitating reinforcement of an ethical culture, which is a very effective compliance control in and of itself.[26]

Research shows that organisations that have an ICS achieve higher CMLs (i.e. Levels 4 and 5) than those that have not. In turn, a higher CML is an important indicator for low or even residual risk of material non-compliances.[27]

Finally, stakeholders (e.g. shareholders, political leadership, regulators, special interest groups, and customers) nowadays demand a high CML, reflected by both legal and ethical conduct. As stated before, an ICS can assist in achieving such CML. Organisations that invest in reaching a high CML are rewarded, not only by a more loyal workforce and customer base, but also by increased opportunities and reduced scrutiny by regulators and

[25] S. Cowly. Wells Fargo Review Finds 1.4 Million More Suspect Accounts. New York Times, 08-31-2017. Available at: https://www.nytimes.com/2017/08/31/business/dealbook/wells-fargo-accounts.html (accessed: March 28, 2020); G. Diepenbrock. Ethics and compliance officers face challenges to their legitimacy, study finds. Phys.Org, 05-18-2017. Available at: https://phys.org/news/2017-05-ethics-compliance-officers-legitimacy.html (accessed: March 28, 2020); B. Blackwelder, et al. The Volkswagen Scandal. Case Study. University of Richmond: Robins School of Business, 01-2016: pp. 1-23. Available at: http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1016&context=robins-case-network (accessed: March 28, 2020).

[26] Antzoulatos-Borgstein, 2017, p. 46; M. Volkov. The Perfect Compliance Combo: Culture and Controls. The Volkov Law Group LLC, 07-30-2017. Available at: https://blog.volkovlaw.com/2017/07/perfect-compliance-combo-culture-controls/ (accessed on: March 28, 2020).

[27] Antzoulatos-Borgstein, 2017, pp. 46-47.

enforcers.[28] Conversely, those who invest, but do not use a matured ICS, run a greater risk of incurring damage.[29]

Relevance and benefits for NATO defence forces.

As applies to companies, there are ample reasons for NATO defence forces to be cognisant of the risks related to holding, using and transferring trade-controlled goods, information and services. The primary risks are as follows and are primarily related to (international, regional, or national) security interests, as well as foreign policy and commercial interests.

Espionage.

Defence information comprises more than classified information. Therefore, targeting of defence information also includes dual-use technology, military critical technology, commercially sensitive data, and proprietary information.[30] Because defence forces hold such a wide range of critical or sensitive information, these organisations are valuable targets for espionage activities.

Economic espionage and theft of trade secrets.

Although traditional espionage may be the most obvious, economic espionage also involves the loss of information to a foreign entity or a competitor. Because a combination of these acts may occur, it is not always easy to draw clear lines between isolated acts of espionage, economic espionage, or trade secret theft. Another difficulty is that these acts take place stealthily, and are therefore by default hard to detect. As revealed in legal cases involving espionage, theft of trade secrets, and trade violations reveal, perpetrators may use different identities, middlemen and shell-companies in order to reveal the true (foreign) end-users of the information or goods obtained.[31]

[28] Antzoulatos-Borgstein 2017; J. Steiner and E. Wollschlager. Compliance Program Strategies for Organization-Wide Accountability. Journal of Health Care Compliance, July-August, 2005: pp. 5-12.
[29] Antzoulatos-Borgstein, 2017, pp. 25-26.
[30] United States Defense Security Service, Center for Development of Security Excellence. Understanding Espionage and National Security Crimes. Counterintelligence Awareness Job Aid Series, 2017. Available at: http://www.cdse.edu/documents/cdse/ci-jobaidseries-understandingespionage.pdf (accessed: March 28, 2020).
[31] United States Department of Justice. Summary of major enforcement, economic espionage, trade secret and embargo-related criminal cases. January 2009 to August 2015, NSD (202) 514-2007. Available at: https://www.pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf (accessed on:

Proliferation.

This does not only relate to the efforts to prevent proliferation of weapons of mass destruction and their technology. Proliferation issues also concern missiles and missile technology, other sensitive technology (either military or dual-use by nature) and even proliferation of small arms. The last is the result of the scale of small arms traffic and the destabilising effect of their trade on international, regional and national security.[32] Also, the rise of transnational terrorism has made stronger and more concerted anti-proliferation efforts.

Since NATO defence forces are end-users of numerous high-technology weapons systems, and sensitive technology platforms related software and technical data, these organisations have a high stake and a shared responsibility to prevent such technology of finding its way to prohibited destinations and prohibited end-users. The fact that the threat is real and proliferators go to great lengths to achieve their objective is reflected by several cases such as the *'Henk Slebos and A.Q. Kahn'* case, concerning the proliferation of numerous controlled nuclear items, dual-use technology and technical data to Pakistan.[33]

Having displayed the main risks for NATO defence forces related to the possession, trade and export of controlled items and technology, the relevance of designing and implementing an ICS may be established. There are two benefits of having an ICS implemented in an organisation. First, laying a foundation for f concerted development and implementation of effective internal trade compliance measures advances the organisation's internal compliance programme and the internal trade compliance function that mitigates trade compliance risks. The second benefit would be the increased trust between NATO allies and subsequent rewards through multinational defence, technology, and logistics cooperation programmes.

Recommendations.

Start with a NATO vision and strategy.

October 27, 2017).

[32] Y. Aubin, Y and A Idiard, A. Export Control Law and Regulations Handbook. A Practical Guide to Military and Dual-Use Goods Trade Restrictions and Compliance. Global Trade Law Series, 2nd ed. Alphen aan den Rijn: Kluwer Law International B.V., 2011: p. 17.

[33] F. Slijper, F. Project Butter Factory. Henk Slebos and the A.Q. Kahn nuclear network. Transnational Institute in association with Campagne tegen Wapenhandel. Amsterdam: Drukkerij Raddraaier B.V., 2007: pp. 32-34.

While it seems self-evident, research shows that not all organisations take a structured, integrated approach to having an integrated compliance strategy. Research also indicates that these organisations run a greater risk to incur material non-compliances and will most probably not exceed CML 4.[34]

Develop and implement a well-balanced integrated compliance strategy (ICS).

Research indicates that a well-balanced ICS provides the best chance for organisations to reach CML 5, and those CML 5 organisations run the least risk to incur material non-compliances.[35]

Focus on the horizon.

Although short term gains, such as boosting profits, boosting quantity and quality of output while driving down costs contribute to measurable success, an overemphasis on such factors can lead to organisational attenuation. For NATO defence forces, this can even lead to security concerns. Therefore, to mitigate the negative side-effects of cost-saving initiatives, focus should be equally on long-term objectives, even when their relationship to profitability (or military effectiveness) is more difficult to measure and quantify. One of these long-term objectives is investment in a well-balanced integrated compliance strategy. Organisations that do so outperform both in terms of compliance and in terms of results.[36]

Beware of the legalistic approach to compliance.

An attitude to trade compliance that is legalistic[37] in nature does not sufficiently protect against the occurrence and consequences of material non-compliances, allegations, and investigations regarding unethical organisational conduct. The main concern with the legalistic approach is that, in most cases, the underlying ethical values, the intent of the regulation or law, and social concerns, are not addressed. When the letter of the law

[34] Antzoulatos-Borgstein, 2017, p. 47.
[35] Antzoulatos-Borgstein, 2017, p. 47.
[36] Antzoulatos-Borgstein, 2017, p. 48.
[37] "Legalistic: strict adherence to law or prescription, especially to the letter rather than the spirit. "Dictionary.com. https://www.dictionary.com/browse/legalistic. "Excessive adherence to law or formula: The resort to legalism has contributed to the present crisis." Oxford Dictionaries. https://premium.oxforddictionaries.com/definition/english/legalism. The main concern with legalistic concepts is the inherent risk of moving away from a law's spirit and ethical or social context, under the guise of strict adherence to legal formula. This, in turn, opens the way to legitimizing the exploitation of legal loopholes, where one knows this is not ethical.

rather than its spirt is emphasized unease can be created with stakeholders that may contribute to actions against the interests of the organisation.

Credibility is key.

Organisations that project sterling images as compliance leaders, while being subject to material non-compliances on a regular basis, risk losing face quickly. Losing credibility can seriously affect relationships with stakeholders, such as regulators. Damaged reputations and relationships can impact an organisation's financial performance or military capability. Therefore, organisations are advised to not only "talk the talk," but also to "walk the walk."[38]

Concluding remarks.

Although, for a while, regulators' focus had been predominantly on commercial organisations, focus has broadened to include international organisations, research facilities, governmental agencies, and their (senior) executives. Specifically, U.S. regulators apply U.S. export controls extraterritorially, thus enabling the targeting of foreign persons, wherever located. This reality makes more relevant the importance of investing in effective compliance measures, including an integrated compliance strategy. Investment in an ICS can lead an organisation to CML 5, which is the best chance for having optimum control and being able to decrease risk exposure to a residual level. Achieving this level risk reduction after compliance controls are applied is crucial for organisations, such as the military forces of the NATO nations, that operate in highly-regulated industries and in high-risk environments.[39]

One of the advantages of an ICS is that it promotes and supports the development and reinforcement of an ethical culture within organisations. An ethical culture, more than 3-S, is an effective instrument to control the effects of human behaviour, which can be capricious at times.[40]

Apart from other benefits, having an integrated compliance strategy, , an effective internal compliance programme, and a professional compliance

[38] Antzoulatos-Borgstein, 2017, p. 49.
[39] Antzoulatos-Borgstein, 2017, pp. 43, 46.
[40] Antzoulatos-Borgstein, 2017, p. 46; M. Volkov. The Perfect Compliance Combo: Culture and Controls. The Volkov Law Group LLC, 07-30-2017. Available at: https://blog.volkovlaw.com/2017/07/perfect-compliance-combo-culture-controls/ (accessed on: March 28, 2020); M. Berzins and F. Sofo. The inability of compliance strategies to prevent collusive conduct. Corporate Governance, 8(5), 2008: pp. 669-680.

function creates trust and enforces credibility with stakeholders. This is not only relevant for for-profit-organisations but also international organizations such as NATO defence forces .

In conclusion, it is stated that further research relating to compliance strategy is welcomed and that this article holds an open invitation for further academic discussion on the topic.

Source: www.act.nato.int

Source: www.act.nato.int

Legal Operations: The Use of Law as an Instrument of Power in the Context of Hybrid Threats and Strategic Competition

by Rodrigo Vázquez Benítez[1]

Introduction

The challenges posed by hybrid threats -and their materialization in Hybrid Warfare and Grey Zone environments- in a context of Strategic Competition have blurred the traditional border between peace and war[2]. This, added to the context of an increased use of asymmetric/non-conventional warfare techniques, both in peacetime, crisis and conflict, and of an enhanced role of (perceived) legitimacy, has made law a particularly

[1] Assistant Legal Advisor at the NATO ACO Office of Legal Affairs of the NATO Supreme Headquarters Allied Powers Europe. The views presented in this article are solely those of the author and do not necessarily represent the views of Headquarters Allied Command Transformation, SHAPE or NATO. The author would like to thank Andrés Muñoz Mosquera, Pavel Kriz and the –former and current- members of the 'legal operations team' whose work and research are the basis and cornerstone of this article.

[2] See Freire 'Strategic Competition and resistance in the 21st century: Irregular, Catastrophic, Traditional and Hybrid Challenges in context' p.19. *See also* A.B. Munoz Mosquera, N. Chalanouli, 'Decoding Gray Zone Environments. Legal Resilience' (2019). Pending Publication. Presented to the University of Exeter – 'Legal Resilience in an Era of Hybrid Threats', 8-10 April 2019.

attractive area to be exploited in conjunction with other instruments of power across the Diplomatic, Intelligence, Military, Economic, Financial, Information and Legal (DIMEFIL) spectrum[3]. This exploitation of what could be defined as the 'legal domain'[4] in a context of strategic competition is referred to by the NATO Allied Command Operations Office of Legal Affairs (ACO OLA) as 'legal operations'[5].

Strategic Competition is a challenge currently felt across all NATO's core tasks. Since 2015, NATO's response to hybrid threats has been focused on improving Alliance situational awareness through intelligence and information sharing, strengthening its deterrence and defense posture[6]. NATO is also enhancing its crisis response procedures to guide decision-making in crises. NATO supports the comprehensive strengthening of Allied resilience to protect our societies and institutions, as well as to deter hybrid attacks by denying their success. These sometimes-preparatory hybrid actions seek to exploit vulnerabilities, precondition and disrupt NATO's ability to take timely decisions, and weaken the Alliance's resilience and ability to withstand or counter a conventional attack. While individual elements or actions may not necessarily be illegal or pose a threat in their own right, when combined they can threaten individual Allies or the Alliance and its cohesion.

The use of hybrid strategies in conflict is not new in human history; what is new for NATO is the way its opponents apply a wide range of political, civil and military instruments in a combined, systematic and coherent manner. These strategies are aimed at particular vulnerabilities of targeted nations and international organizations in order to achieve strategic objectives[7].

[3] 'DIMEFIL' is a concept that refers to the multiple available instruments of state power. *See* K. Oskarsson, R. Barnett. 'The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone' (2017) Open Publications. Volume 1, Num. 2, winter 2017. While DIMEFIL is not an agreed upon NATO term, since 1983 NATO has included these concepts in its *strategic concept / concept stratégique*: **'**The course of action accepted as a result of the estimate of the strategic situation. It is a statement of what is to be done in broad terms sufficiently flexible to permit its use in framing the military, diplomatic, economic, psychological and other measures which stem from it.' See Allied Administrative Publication (AAP-06 2019) NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH), p.121.

[4] On legal domain *see* A. Sari, 'Hybrid Warfare, Law and The Fulda Gap' (2017) *University of Exeter, Law School*, pp. 26-28. *See also* A.B. Munoz Mosquera, Abraham Munoz Bravo, 'The Legal Domain: A Need for Hybrid Warfare Environments' (2017) *A Newsletter of the NATO Legal Community: NATO Legal … matters, issue 2,* December, pp. 9-10.

[5] A. Munoz Mosquera, J.E. Perrin, P. Sergis, R. Vazquez Benitez and B. Montes Toscano, 'The path to Legal Resilience' (2019). Pending Publication. Presented to the University of Exeter – 'Legal Resilience in an Era of Hybrid Threats', 8-10 April 2019.

[6] NATO document, 'Deterrence and Defence' at https://www.nato.int/cps/en/natohq/topics_133127.htm

[7] F. G. Hoffman, 'Conflict in the 21st Century: The Rise of Hybrid Wars' (2007) *Arlington, VA: Potomac Institute*

Furthermore, some hybrid strategies aim at complicating, delaying and eventually impeding timely decision making and undermining the ability of an Ally or the Alliance as a whole to respond to such a threat swiftly, firmly and effectively[8].

In this context, the use of legal operations allows any potential opponent to have a significant impact while avoiding the use of kinetic means, and hence remaining under the threshold of the use of force. Several state and non-state actors are increasingly using the legal domain in a context of strategic competition in order to achieve their strategic objectives and interests, not only tampering with the rules-based international order (RBIO), but also destabilizing international relations.

Legal Operations

Legal operations may be broadly defined as the use of law as an instrument of power. The term encompasses any actions in the legal domain by state or non-state actors aimed at, among others, gaining -or undermining the opponent's- legitimacy, advancing interests, or enhancing/denying capabilities, at the tactical, operational, strategic and/or (geo)political levels. Legal operations may be used across the whole peace-crisis-conflict spectrum through and in combination with a wide range of DIMEFIL tools, not necessarily of a legal nature.

For instance, legal operations may support or materialise a psychological or an information operation against a military commander, by falsely accusing him -inside or outside the courtroom- of committing crimes in the conduct of his duties, or support a broader influence operation, by providing citizenship or pension rights to minorities of a neighbour state. They could also serve to hamper the activities of a competitor or opponent by

for Policy Studies. *See also* "Hybrid warfare can be characterised as a comprehensive strategy based on a broad, complex, adaptive and often highly integrated combination of conventional and unconventional means. It uses overt and covert activities, which can include military, paramilitary, irregular and civilian actors, targeted to achieve (geo) political and strategic objectives. Hybrid warfare is directed at an adversary's vulnerabilities, focused on complicating decision making and conducted across the full spectrum (which can encompass diplomatic, political, information, military, economic, financial, intelligence and legal activity) whilst creating ambiguity and deniability. Hybrid strategies can be applied by both state and non-state actors." Ministry of Defence – Written Evidence submitted to Defence Committee, UK Parliament by S. Bachmann, A.B. Munoz Mosquera, 01 March 2016, <data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/28854.pdf>, 7 December 2018.

[8] A. Munoz Mosquera, S. Bachmann, 'Lawfare in Hybrid wars: the 21st Century Lawfare', *Journal of International Humanitarian Legal Studies 7*, (2016), p. 86.

passing new laws that allow for imposing sanctions on its leadership or embargoes on its assets, or by using international mechanisms to demand responsibility/accountability for its violations of international law. Other instruments of power can be used to change international law itself, by applying diplomatic, political, economic and even military pressure on other actors to accept new practices or interpretations more favourable to the state actor, such as current challenges to the interpretation of the Law of the Sea in particular regions. They may also consist of a 'legal preparation of the battlefield', i.e. actions aimed at shaping in advance the (appearance of) legality or legitimacy of an action normally involving the use of force, minimising the consequences or limiting or delaying retaliation.

Legal operations may thus encompass both the classical legal actions detachable from the conduct of hostilities and those which, on the contrary, are directly or indirectly involved in the achievement of the desired end-effects of an actor against another actor. They can be used as stand-alone actions, in conjunction with other instruments of power, or be part of a wider hybrid or conventional warfare strategy.

As opposed to legal operations, the commonly used term *Lawfare* is defined as "the strategy of using -or misusing- law as a substitute for traditional military means to achieve a warfighting objective."[9] Although this concept is often used to describe some of the actions encompassed by the term 'legal operations,' it is less comprehensive, more limited in scope, and the object of academic controversies[10].

The Preservation of the Rule of Law

As a result of NATO's commitment to countering hybrid threats, ACO OLA has recognised the need to anticipate, detect, identify, assess and respond to hostile legal operations through a uniformed methodology while recognizing the sovereign powers of the Allies, embracing the rule of law, and stressing the importance of a stable international legal framework. The latter are particularly relevant.

As expressed in the preamble to the North Atlantic Treaty, the NATO Allies are "determined to safeguard the freedom, common heritage and

[9] A contraction of the words 'law' and 'warfare', lawfare is an academic concept developed by Maj. Gen. (Ret.) Charles Dunlap over the years 2001-2011. *See* C. Dunlap, 'Lawfare today: A perspective', *Yale Journal of International Affairs* (2008), p. 146-154.

[10] For instance, see Wouter G Werner, 'The Curious Career of Lawfare' (2010) 43 *Case W Res J Int'l L* 61.

civilisation of their peoples, founded on the principles of democracy, individual liberty *and the rule of law*." The preservation of the rule of law and a stable RBIO is thus one of the underpinning values of the Alliance.

Legal operations is a neutral concept, in the sense that their use might not necessarily entail an illegitimate use of the law. For instance, using or enhancing the law to enforce currently existing prohibitions, using domestic or international courts to demand responsibility/accountability for violations of the law, or passing new legislation or adopting new international instruments with the aim of preventing further breaches or erosion of the rule of law or the RBIO, represent what could be categorised as 'white' legal operations; this is, the use of law as an instrument of power not to challenge our values-based system, but to reinforce it.

Nonetheless, the use of law as an instrument of power does carry the risk of eroding the rule of law and, hence, any activities in the legal domain by the Allies must always look carefully at the overall system and how their individual and collective actions -not necessarily using the legal instrument of power- affect the integrity of the rule of law and the stability of the RBIO.

Operationalisation

Departing from the concept of legal operations, the methodological framework used by ACO OLA for its analysis is the 'Legal Operations Response Cycle' (LORC). Broadly, the response cycle is composed of four main phases to be followed when facing –to defend against- any given hostile legal operation: Identification; Assessment; Strategy Definition; and Response. However, the LORC is only a process that needs to be integrated into, and supported by, wider processes, effective actions and tools in order to achieve success.

In this sense, legal vigilance is essential for the detection at an early stage of hostile legal operations and their potential effects before they are fully displayed. Moreover, legal operations, like other activities in hybrid environments, are characterized by the need to include in their identification, assessment and response a variety of actors within all instruments of power in the DIMEFIL spectrum. These would need to 'interoperate' when assessing or responding to a hostile legal operation. For this reason, legal operations form part of planning, training and exercising, which is essential for the awareness and readiness of all actors potentially involved, and contributes to increasing NATO's resilience and deterrence posture.

These activities underpin ACO OLA's efforts in the field of legal operations, having in legal vigilance its main effort and the preservation of the RBIO and the rule of law at its core.

Conclusion

The use of law as an effective instrument of power is not a new phenomenon, as demonstrated by the success of Hugo Grotius' *Mare Liberum*: In 1493, Pope Alexander VI used a papal decree to divide the world's newly discovered continents and oceans between Spain and Portugal.[11] By the 17th Century, Portugal's sovereign control over parts of the Atlantic and Indian Oceans gave it a monopoly on the East India trade. Not being able to confront militarily the mighty Portuguese navy, and in order to challenge its monopoly, the Dutch East India Company hired the scholar Hugo Grotius, who developed a new legal doctrine advocating for the freedom of oceanic navigation[12]. This new doctrine was published in *Mare Liberum* (Freedom of the Seas) in 1609[13] and intensely promoted by the Dutch East India Company. Grotius' novel arguments, which laid the foundations of the modern law of the sea, immensely benefited the Dutch East India Company, were accepted and remain controlling to this day[14].

Our times face similar novelty. Traditional, kinetic deterrence is so successful that state and non-state actors are engaging in new, hybrid tactics in order to compete below the threshold of armed conflict. Moreover, perceptions of legality and legitimacy have gained renewed importance due to the effects of globalisation and almost ubiquitous public and personal access to information and opinion. Strategic competition has thus highlighted the relevance of law as an essential instrument of power amongst the other instruments in the DIMEFIL spectrum. NATO's opponents, state and non-state actors, use legal operations extensively across the spectrum of peace to war

[11] The decree was issued on September 26, 1493 and then modified in 1494 by the Treaty of Tordesillas. See J. A. Martínez Torres «Gobernar el Mundo». La polémica *Mare Liberum* versus *Mare Clausum* en las Indias Orientales (1603-1625) *Anuario de Estudios Americanos*, Vol 74, No 1 (2017); *see also* footnote 97, Christopher R Rossi, 'Treaty of Tordesillas Syndrome: Sovereignty ad Absurdum and the South China Sea Arbitration' (2017) 50 *Cornell Int'l LJ* 231, 244-245.

[12] *Ibid.*

[13] *The Free Sea*, Hugo Grotius, translated by Richard Hakluyt, Edited and with an Introduction by David Armitage, Liberty Fund, Inc.,(2004) Indianapolis, p13.

[14] "Article 89" Invalidity of claims of sovereignty over the high seas "No State may validly purport to subject any part of the high seas to its sovereignty." *United Nations. Law of the Sea: Navigation on the High Seas: Legislative History of Part VII, Section I (Articles 87, 89, 90-94, 96-98) of the United Nations Convention on the Law of the Sea.* (1989) New York, United Nations. p.1.

all over the globe.

Consequently, the Allies must be vigilant and work individually and collectively to detect where its competitors are instrumentalising and undermining the RBIO. As they pledged in the preamble of the North Atlantic Treaty, they must work actively to strengthen and safeguard our rule of law system, denying the advantages that competitors can obtain by using instruments of power under -and above- the threshold of armed conflict. In order to achieve this effect, legal operations response, vigilance, training and awareness are essential activities that NATO and its members should undertake and integrate in their tasks and processes, with the ultimate aim of preserving the Alliance's resilience, strengthening its defence and deterrence posture, and supporting and protecting the fulfilment of its purpose.

***

The names of the Belgian, Dutch and German contractors displayed at the entrance of the construction site of the temporary NATO HQ in Brussels in November 1966.

Source: https://www.nato.int/cps/en/natohq/declassified_147208.htm

The Road to Hell is Paved with Bad Contractors: Vendor Vetting is a Better Path

by Brett Sander[1]

Every North Atlantic Treaty Organization (NATO) contracting professional needs their legal representative in supply chain oversight meetings. Hunt down your legal advisor or fill up their calendar with meeting invitations. Once you read about overcoming challenges within the US Central Command (CENTCOM) supply chain management in Afghanistan, you will realize why.

[1] Brett Sander is a US legal practitioner and principal at Vendor Clearance LLC where he advises government contractors on developing robust internal controls. Prior to private practice, he served as a US Army judge advocate. His assignment at Task Force 2010, a US Central Command unit tasked with vetting contractors in Afghanistan, is the inspiration for this article. The views expressed in this article are solely those of the author and may not necessarily represent the agreed upon views of NATO, ACO or ACT.

Before jumping to Afghanistan and supply chain compliance, we discuss the legal department's role in an organization. Senior leadership in government, industry, and international organizations reach out to the legal department for reviewing contracts and settling contract disputes. But the legal department's primary task is to mitigate the organization's risk. Hence, the emergence of the Chief Compliance Officer in many legal departments, or as I think better named the "Chief of Risk Mitigation".[2]

From a US point of view, risk mitigation failed in Afghanistan in 2010. The US Congress investigated CENTCOM's contracting and released a report titled "Warlord, Inc." The report is a damning analysis of lack of supervision of a $2.16 billion contract. CENTCOM units ignored reports of demands by Afghan warlords for bribes from contractors for safe passage on Afghanistan's highways. From the report:

> "The 484th Joint Movement Control Battalion was responsible for managing and overseeing HNT[3] missions from May 2009 (when the contract started) to February 2010. According to Lieutenant Colonel David Elwell, the commander of the 484th, no one in the battalion ever personally witnessed trucking operations 'outside the wire' – outside of the major airfields and forward operating bases where supplies are uploaded and downloaded. The 484th did not have the 'force structure, the equipment, or the security' to put eyes on the road. 'It would have been a combat mission'".[4]

NATO decision-makers cannot overlook the risks they face from their supply chain. Recent conflicts and peacekeeping missions are rife with contractor scandals involving human rights abuses,[5] sexual assault and trafficking[6] and destabilization of the health of local communities.[7]

---

[2] US Department of Justice recognizes the necessity of this position within a company. *See* US Department of Justice Criminal Division, 'Evaluation of Corporate Compliance Programs, (Updated April 2019)' 11 <https://www.justice.gov/criminal-fraud/page/file/937501/download> accessed 15 May 2020

[3] U.S. Department of Defense's Host Nation Trucking (HNT) contract.

[4] Warlord, Inc., Extortion and Corruption Along the U.S. Supply Chain in Afghanistan, H.R. Subcomm. on Nat'l Sec. and Foreign Affairs, H.R. Committee on Oversight and Gov't Reform (2010) 49 [hereinafter Warlord, Inc.]

[5] Katherine Hawkins, 'CACI's Forgotten Role in Abu Ghraib (I)' (*Huffpost*, 29 October 2013) <https://www.huffpost.com/entry/cacis-forgotten-role-in-a_b_3830280https://www.huffpost.com/entry/cacis-forgotten-role-in-a_b_3830280> accessed 8 May 2020.

[6] Ed Vulliamy, 'Has the UN learned lessons of Bosnian sex slavery revealed in Rachel Weisz Film?' (*Guardian*, 14 January 2012) <https://www.theguardian.com/world/2012/jan/15/bosnia-sex-trafficking-whistleblower> accessed 8 May 2020

[7] Camila Domonoske, 'U.N. Admits Role in Haiti Cholera Outbreak That Has Killed Thousands' (*National Public*

I. The Proposal:

I recommend NATO create a vendor vetting system to deny issuance of awards to contractors that pose force protection and reputational risks. This innovation will benefit host nations such as Afghanistan by preventing NATO funding of criminal or other maligned actors. This also protects NATO, itself, from using contractors connected to insurgent forces, criminal elements or foreign intelligence.

II. Nomenclature in Article

The term "contractor" refers to any company that provides goods or services under a contract with a governmental or intergovernmental agency. This term does not refer to employees of the company.

The term "vendor vetting system" and "vetting system" refers to the proposed compliance mechanism for NATO to review contractors. The "Vendor Vetting Program" refers to the specific system established by CENTCOM in Afghanistan to screen Department of Defense contractors for links to force protection risks.[8]

The references to "CENTCOM" include all subordinate commands. United States Forces - Afghanistan is the prime CENTCOM subordinate command in Afghanistan. I also refer to Task Force 2010 "TF2010", a CENTCOM unit that shaped and managed the Vendor Vetting Program for several years.[9]

The terms "barment" and "ban" describe CENTCOM's action of preventing a contractor from receiving eligibility for contracts under the Vendor Vetting Program. Barment is not to be confused with formal "debarment" — a process many federal governments and agencies use to exclude a government contractor from contracting opportunities for a set length of time.

III. Adopting CENTCOM'S Risk Mitigation Process

Radio, 18 August 2016) <https://www.npr.org/sections/thetwo-way/2016/08/18/490468640/u-n-admits-role-in-haiti-cholera-outbreak-that-has-killed-thousands> accessed 8 May 2020

[8] CENTCOM has expanded the Vendor Vetting Program to cover other countries within the CENTCOM region since the author left the Army

[9] CENTCOM has relocated the Vendor Vetting Program to MacDill Air Force Base since the author was a member of TF2010. *See* OFFICE OF THE DEPUTY ASSISTANT SEC'Y OF DEF., CENTCOM QUARTERLY CONTRACTOR CENSUS REPORT (October 2018) <https://www.acq.osd.mil/log/PS/CENTCOM_reports.html> accessed 8 May 2020

This article explores CENTCOM's compliance approach and discussion points for NATO to consider for replicating this undertaking. CENTCOM's Vendor Vetting Program began under a subordinate contracting command. The Program next moved to TF2010, a CENTCOM anti-corruption unit.[10] It was unclear whether the Program was a contracting tool, a force protection tool, or a little of both. Due the confluence of an urgent need for a vendor vetting system and reduction of troops in Afghanistan, CENTCOM did not resolve these questions. This ambiguity led to shortcomings in the Vendor Vetting Program which this article explores. Ultimately, the Vendor Vetting Program is both of these things, and a potential means to aid contractors to create their own internal compliance tools.

All large organizations operating in conflict areas face a repeat of the CENTCOM trucking disaster. Failure to take preventive action can land an organization on the front pages of *Le Monde* or the *Wall Street Journal*. Starting with its presence in Bosnia, NATO has undertaken several missions in similar environments including operations in Afghanistan, Kosovo, Pakistan, and Libya. A NATO presence requires responsible contractors to support the mission. Hence, the urgency I encourage NATO to exert to establish its own vendor vetting system.

IV. Vendor Vetting Program in Action

The Vendor Vetting Program, run by TF2010 for several years, was a novel way for U.S. and Coalition base commanders to screen contractors prior to contract award. The Program took advantage of a DOD database, the Joint Contingency Contracting System (JCCS). JCCS requires all potential contractors to register and upload in-depth information including their owners, key personnel, and financial particulars. After review of intelligence from the field and JCCS data, the Program's intelligence analysts made recommendations on a contractor's links to bad actors or other force protection risks. TF2010 reviewed contractors and forwarded recommendations to a decision-maker (usually a general officer). The decision-maker either granted or denied base access to the contractors. A contractor must receive base access as a prerequisite to receive a

[10] Confirmed by email between former TF2010 Director and author (20 February 2020); *See* OFFICE OF THE DEPUTY ASSISTANT SEC'Y OF DEF., CENTCOM QUARTERLY CONTRACTOR CENSUS REPORT (January 2012) <https://www.acq.osd.mil/log/PS/CENTCOM_reports.html> accessed 8 May 2020 (TF2010 was established "to more effectively link US contracting dollars to a winning [counterinsurgency "COIN"] strategy in Afghanistan" and "ensure that the billions of US dollars being spent are used as an effective tool")

CENTCOM contract.[11]

This due diligence protected CENTCOM from further negative Congressional investigations and headlines stories regarding supply chain connections to warlords and insurgents. While I was with TF2010, I observed only one contractor that made headline news after CENTCOM implemented the Program.[12]

Based on my work at TF2010, I made the following observations:

1. Relying on OFAC/SAM/UN Sanctions/EU Financial Sanctions is not sufficient to vet potential contractors in conflict environments. Most contractors banned by CENTCOM were not banned or debarred in other systems;
2. A vetting system with minimal administrative processes and hurdles is necessary to meet acquisition needs;
3. An intelligence-based program may exclude contractors who only have casual links to bad actor(s). An organization must accept this risk to keep up with the need for speedy battlefield procurement;
4. Decision-makers must consider political and economic effects when developing a vendor vetting system. CENTCOM attempted to ban Kam Air, a company linked to former President Hamid Karzai. This endeavor proved to be embarrassing for CENTCOM. Even if a ban is merited, an organization must consider non-security factors in each vetting decision.[13]

V. Intricacies of the Vendor Vetting Program

This section explores several components that served as the building blocks for CENTCOM's Program.

[11] *See*, *e.g.*, NCL Logistics Co. v. United States, 109 Fed. Cl. 596, 618 (2012); Afghan Premier Logistics, B-409971, 2014 U.S. Comp. Gen. LEXIS 279 (Comp. Gen. September 26, 2014); Aria Target Logistics Serv., B-408308.23, 2014 WL 4363483 (Comp. Gen. August 22, 2014)

[12] Zurmat Material Testing Laboratory continued to receive contracts even though CENTCOM previously banned its parent company Zurmat Group from receiving contracts. *See* Matthew Rosenberg, 'Afghan Companies with Insurgent Ties Still Receive U.S. Contracts' (*N.Y. Times*, 13 November 13, 2013) <https://www.nytimes.com/2013/11/13/world/asia/afghan-companies-with-insurgent-ties-still-receive-us-contracts.html?searchResultPosition=1> accessed 9 May 2020.

[13] Dan Murphy, 'Afghan Corruption, Opium and the Strange Case of Kam Air' (*Christian Science Monitor*, 5 February 2013) <https://www.csmonitor.com/World/Security-Watch/Backchannels/2013/0205/Afghan-corruption-opium-and-the-strange-case-of-Kam-Airhttps://www.csmonitor.com/World/Security-Watch/Backchannels/2013/0205/Afghan-corruption-opium-and-the-strange-case-of-Kam-Air> accessed 9 May 2020

A. Risk Categories

Planners must establish risk categories for effective contractor vetting. In Afghanistan, TF2010 categorized contractors with risk ratings of moderate, significant, high or extremely high.[14] Contractors with ties to the Taliban, insurgents, criminal activity, and foreign intelligence received a "high" or "extremely high" risk rating.[15] Those assigned either of these two latter ratings may not receive a CENTCOM contract unless issued an exception to policy.[16]

These rules do not have to be rigid. Planners may adjust requirements based on the risk tolerance of the organization. For example, in certain situations, an organization may only allow contractors with a "moderate risk" rating to receive contracts. In addition to capturing an organization's acceptable risk appetite, the classification process must be understandable by the implementing staff. Otherwise, the system will not serve the rapid pace of contract procurement.

Here is a risk categories table (abridged for this article)[17]:

Moderate Risk	**Significant Risk**	**High Risk**	**Extremely High Risk**
Local company with excellent internal controls and no recent security/base violations	New local company with limited internal compliance	Key personnel worked for company banned by NATO or other governments	Owner or company had prior transactions with individuals or organizations on a recognized sanctions list
Long-term NATO contractor with excellent internal controls and no recent security/base violations	Long-term NATO contractor whose lower level employees have violated minor base regulations	Intelligence shows owner had several prior meetings with warlords or foreign intelligence	Owners convicted of fraudulent activity related to government procurement

[14] *NCL Logistics Co.*, 109 Fed. Cl. At 608
[15] Afghan Premier Logistics, B-409971, 2014 U.S. Comp. Gen. LEXIS 279 at *3 (Comp. Gen. September 26, 2014)
[16] *Id*.
[17] Chart not based on TF2010 internal documents

	(possession of alcohol or other contraband)	agents (unknown what was discussed during meeting)	

B. Intelligence Basis

To identify contractors who pose force protection risks, TF2010 relied on intelligence collected by the US.[18] In addition, the analysts reviewed information contractors provided to the JCCS website. To bid on contracts, CENTCOM required contractors to upload details on their owners, key personnel, subcontractors, and financials to JCCS. Like a large puzzle, the TF2010 intelligence team pieced together these bits of information to draw connections between the contractors and bad actors (e.g. warlords, insurgents, criminals, foreign intelligence). The goal was to evaluate collected intelligence in a consistent manner. Resources such as the Department of the Army Field Manual FM 2-22.3 (Human Intelligence Collector Operations) can guide analysts on the reliability and weight to give to the intelligence they receive:[19]

Source Reliability

A	**Reliable**	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability
B	**Usually Reliable**	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	**Fairly Reliable**	**Doubt** of authenticity, trustworthiness, or competency but has provided valid information in the past
D	**Not Usually Reliable**	**Significant doubt** about authenticity, trustworthiness, or competency but has provided valid information in the past
E	**Unreliable**	**Lacking** in authenticity, trustworthiness, and

[18] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-335 U.S. EFFORTS TO VET NON-U.S. VENDORS NEED IMPROVEMENT n.8 (2011); Author cannot delve further into intelligence collection methods

[19] U.S. DEP'T OF ARMY, FIELD MANUAL, 2-22.3, HUMAN INTELLIGENCE COLLECTOR OPERATIONS app. B-1 (6 Sep. 2006)

		competency; history of invalid information
F	**Cannot Be Judged**	**No basis** exists for evaluating the reliability of the source

Information Content

1	**Confirmed**	**Confirmed** by other independent sources; **logical** in itself; Consistent with other information on the subject
2	**Probably True**	Not confirmed; **logical** in itself; **consistent** with other information on the subject
3	**Possibly True**	Not confirmed; **reasonably logical** in itself; **agrees with some** other information on the subject
4	**Doubtfully True**	Not confirmed; possible but **not logical**; **no other information** on the subject
5	**Improbable**	Not confirmed; **not logical** in itself; **contradicted** by other information on the subject
6	**Cannot Be Judged**	**No basis** exists for evaluating the validity of the information

Each piece of intelligence receives a rating based on an evaluation of the source reliability and the information content. The rating drives the intelligence team's recommendations. For example, a team may accept that a contractor is linked to an insurgent based on human intelligence with an A1 intelligence rating but will require two pieces of intelligence with a rating of C3 to confirm the same link. An organization that cannot rate the intelligence it reviews opens the door to an erratic process and inconsistent results.

C. Evidentiary Standard

The organization must also establish an evidentiary standard to limit arbitrary and capricious decisions. This may be situation dependent. Where intelligence is limited but risks are high, an organization may use a lower burden such as proof by reasonable suspicion. For example, the contractor is part of a small trade association that has several known bad actors as members. Where the overall risk is low or reliable intelligence exists, an organization may raise the standard to preponderance of the evidence or

even probable cause.[20]

TF2010 sought to ensure that the burden of proof was not so low as to risk litigation or the reputational risk to the process. I alluded to CENTCOM's attempt to ban Kam Air, the principal Afghan airline company. CENTCOM suspected Kam Air of transporting large quantities of opium inside and outside of the country.[21] Following the Kam Air barment, President Hamid Karzai's office demanded evidence from the U.S. military, to conduct its own investigation.[22] This put US Forces in a conundrum since the evidence was likely intelligence-based.[23] Within one month of the barment, the United States government reversed course and allowed Kam Air to bid on future contracts.[24] Any organization will have to navigate such occasional political challenges. A consistent evidentiary protocol helps the system overcome outside objections that question the fairness of the vetting decisions.[25]

Further, standardized burdens of proof mitigate occurrences of arbitrary decisions from internal pressures. Whether caused by staff turnover or actual favoritism by vetting decision-makers, such requirements best protect the integrity of a vendor vetting system from internal ambiguity or corruption.

D. Collecting the Intelligence

A vetting program can only function if it actively gathers intelligence on potential contractors, their owners, and key personnel. Otherwise, the program is relying on inadequate OFAC/UN/Interpol/EU sanctions lists. These sanctions lists failed to identify contractors later barred by the Vendor Vetting Program.

An organization must establish the relations and develop the procedures to collect intelligence. TF2010 had the fortune to rely on intelligence

[20] By way of illustration, reliable intelligence indicating that the company has actually entered into business transactions with a bad actor

[21] Alissa J. Rubin, 'Afghans Bristle at U.S. Ban on Airline' (*N.Y. Times*, 30 January 2013) <https://www.nytimes.com/2013/01/31/world/asia/afghanistan-bristles-at-us-ban-on-kam-air-airline.html?register=email&auth=register-email> accessed 9 May 2020

[22] *Id*.

[23] Susan Cornwell, 'U.S. Army Won't Bar Contractors Linked to Afghan Insurgents - Watchdog' (*Reuters*, 30 July 2013) < https://uk.mobile.reuters.com/article/amp/idUKBRE96T04P20130730> accessed 9 May 2020

[24] Heidi Vogt, US military Lifts Ban on Afghan Airline' (*Yahoo News*, 5 Feb. 2013) <https://news.yahoo.com/us-military-lifts-ban-afghan-064431818.html> accessed 9 May 2020

[25] Author was not part of the Kam Air barment or subsequent barment lifting. Author does not have knowledge if a more thorough investigation by the US or an established burden of proof would have changed the later course of action to lift the barment.

accumulated by the U.S. who held a significant footprint in Afghanistan. However, this may not exist in every conflict or peacekeeping mission.

This article will not delve into intelligence collection and sharing at NATO. While a NATO outsider, I recognize that challenges exist at NATO where Members may only share limited intelligence within the organization or between Members. A Chief of Risk Mitigation should encourage a "need to share" attitude as opposed to a "need to know"---an issue that continues to impede NATO's internal structures.[26] In 2017, NATO created the Joint Intelligence and Security Division ("JISD").[27] JISD is most likely the right place to house the intelligence team for the vetting system.[28] The Vendor Vetting Program benefited from several countries sharing intelligence.[29] The Chief of Risk Mitigation should encourage "need to share" from potential intelligence contributors while also recognizing the contributors' national caveats and political limitations. In addition, NATO should not ignore intelligence opportunities from interviewing the employees of current and potential contractors. A successful vetting system requires actionable intelligence from the field. The organizations that sit behind a computer and rely on newspaper headlines/commercial databases will not achieve the necessary intelligence collection for a robust vetting system.[30]

VI. AREAS FOR IMPROVEMENT AND CONSIDERATION

A. Question of Transparency

CENTCOM made a strategic decision to maintain a non-transparent vetting system. Specifically, CENTCOM instructed contracting officers not to reveal category ratings and base access barments to contractors except in limited situations.[31] This decision is in contrast to the 841 process, another vetting system CENTCOM chose not to rely on, which publicly listed barred

[26] Arndt Freytag von Loringhoven, 'A New Era for NATO Intelligence' (*NATO Review*, 29 October 2019) <https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html> accessed 9 May 2020

[27] *Id*.

[28] Arndt Freytag von Loringhoven, 'Adapting NATO intelligence in support of "One NATO"' (*NATO Review*, 8 September 2017) <https://www.nato.int/docu/review/2017/Also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/EN/index.html> accessed 9 May 2020

[29] US military benefits from sharing information with four other close allies; *See* Scarlet Kim and Paulina Perlin, 'Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance' (*Lawfare*, 25 March 2019) <https://www.lawfareblog.com/newly-disclosed-nsa-documents-shed-further-light-five-eyes-alliance> accessed May 11, 2020

[30] Warlord, Inc., *supra* note 2, at 49

[31] *See NCL Logistics Co.*, 109 Fed. Cl. 596 at 621

contractors in Afghanistan.[32] I was not part of the decision to conceal the identities of the barred contractors but suspect it was to protect classified intelligence. Keeping the barment list classified has three negative consequences:

1) It impedes a barred contractor's ability to take steps to improve its internal controls (informing a contractor that it is barred can prod contractor to take rehabilitative action);
2) Other contractors risk the chance of conducting business with the barred contractor and could damage their own reputations;
3) It creates unnecessary divisiveness and distrust between the organization and contractors.

An organization should weigh maintaining an open-door relationship with contractors against the possibility that disclosing the list of barred contractors will reveal classified information. As NATO grows more dependent on contractors for logistics, I contend the former option will serve NATO and its contractors better in the long-run.

B. Right to Confront/Appeal

CENTCOM avoided a formal debarment program with extensive due process because it prioritized efficiency and protection of classified evidence.[33] However, it neglects fairness. A barred contractor's right to appeal dovetails with the discussion on system transparency. Again, the recommendation is for a system of trust with the contractors by allowing barred contractors to appeal.

Normally, in US government contracting, an agency may only bar contractors from receiving government contracts if it affords the contractors some due process that ensures "fair and uniform" treatment.[34] The Vendor Vetting Program, however, does not have a true appeal process. This creates two serious issues. First, good contractors can be unfairly denied contracting opportunities and have minimal recourse. Second, political contacts and

[32] *See* list at https://www.acq.osd.mil/dpap/pacc/cc/docs/Identified_Enemy_List_consolidated.pdf accessed 10 May 2020

[33] The US Court of Federal Claims opined contractors in Afghanistan are not afforded traditional due process rights due national security issues the US faces. *See MG Altus Apache Co.*, 111 Fed. Cl 425 at 445

[34] Gonzales v. Freeman, 334 F.2d 570, 480 (D.C. Cir. 1964); *See also* (Horne Brothers v. Laird, 463 F.2d 1268, 1270 (D.C. Cir. 1972) (held US Department of Defense must afford some due process to a contractor for a "protracted" suspension); *See also* FAR 9.406 (controlling regulation for debarment for many contracting agencies)

former general officers will lobby CENTCOM to allow a contractor back on base. [35] This creates unnecessary pressure on action officers to change determinations based upon political pressure, as opposed to available intelligence.[36] From a former TF 2010 Director, I learned that there was an interest to create an appeals process but staff turnover hampered efforts to make significant change.[37] NATO's vendor vetting should avoid TF2010's shortcomings and develop an appeals process, even if it only affords limited due process. Like issues of transparency, fairness to the contractors will ultimately benefit NATO.

C. Opportunity to Educate Contractors

The Vendor Vetting Program does not educate contractors concerning best practices to maintain base access.[38] I recommend that NATO establish an educational arm that informs contractors on good internal controls and policy development.

In my private practice, I have advised clients banned by the Vendor Vetting Program to establish a chief of compliance position and follow recommendations in the U.S. Department of Justice's Evaluation of Corporate Compliance Programs. Clients have strengthened their supply chain management system through using third-party vendors to screen their subcontractors and suppliers by searching sanctions databases and criminal convictions. They have also engaged organizations such as TRACE International,[39] a leading international anti-corruption business association , to develop stronger codes of conduct and implement anti-bribery training.

Similarly, NATO's vendor vetting system should provide guidance to contractors to strengthen internal oversight. NATO might even require a code of conduct and a whistleblower reporting system for companies of a certain size.[40] A proactive role by NATO requiring contractors to adopt such internal controls would both reduce contractor corruption and open doors between NATO and the contractors' internal compliance teams.

---

[35] Observed by other former TF2010 members in multiple discussion with the author (2013 – 2020)
[36] *Id.*
[37] Confirmed by email between former TF2010 Director and author (9 May 2019)
[38] Original JCCS website had small section on fraud awareness but no other information on best practices; Current JCCS website has no information on such practices <www.jccs.gov> accessed 15 May 2020
[39] "TRACE membership and due diligence services are designed to help companies spend less while maintaining a dynamic anti-bribery compliance program." See Trace International at https://traceinternational.org
[40] *See* FAR 3.908 and 3.10 (these items required in certain US Department of Defense contracts)

D. Housing Vendor Vetting System

NATO has several different agencies and organizations, each with their own procurement systems. I recommend that NATO centralize its vendor vetting system and require all NATO agencies to screen their contractors through it. To avoid potential conflicts of interest, CENTCOM purposely placed the Vendor Vetting Program away from the contracting officers. CENTCOM recognized that contracting officers focus on acquiring goods and supplies at the best value rather than force protection or other risk mitigation requirements. Contracting officers are not privy to the internal-decision process of TF2010. If an agency wanted to use a barred contractor, the agency/military command made a special request through the Vendor Vetting Program.[41] CENTCOM reviewed the request and only allowed use of a barred contractor under unique conditions.[42]

Similarly, NATO can manage a vendor vetting system that has checks and balances to issue appropriate decisions based on NATO's operation needs. The system could comprise of the following:

- **Vendor Vetting Board** – This board makes the ultimate decision on the acceptability of proposed contractors to provide goods and services for NATO based on recommendations from the Vendor Vetting Office. The board members function independent of the day-to-day operations of NATO's vendor vetting office. I recommend that board members come from different departments within NATO and have a rank of OF-7 minimum or its civilian equivalence. The Vendor Vetting Board can use rotating members. The Board can also review exception to policy requests from NATO commanders/agencies.[43]

- **Chief of Risk Mitigation** – This advisor has a legal or compliance background and the necessary rank to effectively guide the Vender Vetting Board and the Vendor Vetting Office. Duties consist of ensuring that NATO's vetting system operates in a consistent and reasonable manner. This individual will also advise NATO leaders on the rationale for previous decisions of the Vendor Vetting Board as needed. A high-ranking official from the Office of Legal Affairs may best serve this

[41] *MG Altus Apache Co.*, 111 Fed. Cl at 436
[42] *Id*.
[43] NATO may consider also creating an appeals process for banned contractors that appeals to a higher authority level

position.

- **Vendor Vetting Office** –The Vendor Vetting Office provides the day-to-day review of contractors for use by NATO agencies. This office develops the procedures for effective and efficient vetting. Ultimately, this office will present the list of contractors to the Vendor Vetting Board with recommendations on approving or disapproving each contractor. Some positions that can best support this office:
    - Operations Director (Manages vetting program)
    - Legal Advisor (Advises Director on the legal sufficiency of each recommendation in accordance with internal procedures)
    - Intelligence Chief (Explains analyses of intelligence collected by JISD and other sources)
    - Force Protection Officer (Provides assessment of contractor's risk to NATO Forces)
    - Procurement Officer (Provides guidance on procurement challenges if a contractor is banned; serves as liaison to contracting officers of NATO agencies)
- **Contractor Guidance Center (Educational Arm)** –NATO may consider an office that aids contractors to incorporate internal controls, conflict of interest training and other best industry practices. These concepts may be new for contractors in certain environments. Such preventative steps will benefit both the contractors and NATO. These constructive steps can also open the door for contractors to disclose fraud, waste and abuse to NATO officials. To avoid unintended bias, the Contractor Guidance Center should not be privy to the classified information reviewed by the Vendor Vetting Office.

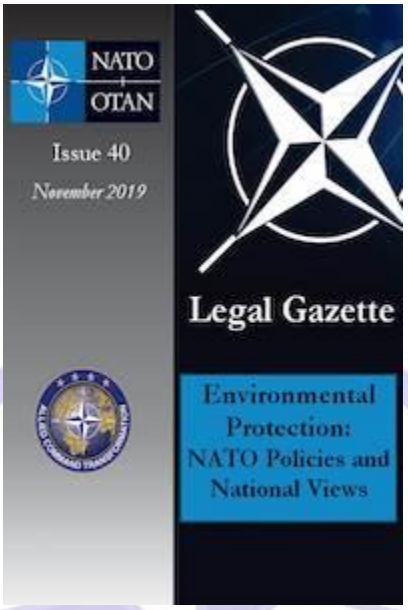
VII. Final Thoughts

Contingency actions often require long supply chains to sustain multinational forces. Most armies must subcontract such logistics operations out to private companies due to the tremendous needs of military units and the high risks of moving supplies in a foreign environment. Organizations like NATO cannot ignore that these private companies become an extension of the multinational forces. Negative actions by the companies endanger troop safety and objectives. A strong compliance system that continually scrutinizing such companies through vendor vetting is mandatory to avoid scandals and inadvertent financial contributions to bad actors. This is the

better path for NATO to follow to avoid the road travelled by bad contractors.

***

...of NOTE



The NATO Legal Gazette can be found at the official ACT web page:
http://www.act.nato.int/publications

and at LAWFAS