# The Future and Ethics of
# Uncrewed and Autonomous Warfare

# GNSI Tampa Summit 2

SEPTEMBER 27-28 2023 // UNIVERSITY OF SOUTH FLORIDA

**Authored By:**
Arman Mahmoudian

# — SUMMIT REPORT —

GNSI TAMPA SUMMIT 2

Foreign Defense Partnerships in a Global Competitive Market

GLOBAL & NATIONAL SECURITY INSTITUTE
TAMPA SUMMIT

# ★ ★ ★ ★
# The 4-Star Review

*Insights and observations from General McKenzie, who served from 2019 - 2022 as Commander of United States Central Command (USCENTCOM)*

One of the key takeaways from GNSI Tampa Summit 2, featuring the 8th Great Power Competition Conference, confirms something I've suspected for a long time: the next war will be driven by information. Collecting information, processing it, using it efficiently, and denying an adversary's ability to do the same will be the central calculus of that war.

*GNSI Tampa Summit 2: The Future and Ethics of Uncrewed and Autonomous Warfare* laid out in great detail the relentless march of technologically advanced warfare. As we've seen in the Russian/ Ukraine war, as well as in Gaza and other areas of conflict in the Central Command Region, uncrewed and autonomous weapons systems, especially drones, have significantly redistributed power in warfare.

As you'll read in this report, these autonomous systems, featuring artificial intelligence, machine learning, and other adaptive technologies, are redefining combat and military training. We're witnessing a shift from centralized command structures to more autonomous operations that must be able to function in an information-denied environment. AI's ability to process overwhelming data, and its integration into military operations is transforming modern warfare, with a focus on enhancing decision-making and operational efficiency.

As these advanced technologies take on an increasingly important role in the world's arsenals, demanding more and more information to function, it's becoming increasingly difficult to collect that information under battlefield conditions. Disrupting the flow of information to these systems dramatically limits their effectiveness. The ability to secure our own systems is as vital as being able to disrupt our adversary's systems.

The ability to disrupt and cause chaos is inherently easier and stronger than the ability to cohere and bring things together. That's been true for hundreds of years on the battlefield. But these advanced systems, autonomous, and semi-autonomous, are making it easier to disrupt than ever before.

Such technology has democratized these new weapons. No longer are these systems the purview of global superpowers. Nearly any group intending to wreak havoc can wield these weapons with minimal budgets and off-the-shelf components. These types of weapon systems give an asymmetric advantage to lesser powers and non-state entities as they seek to disproportionally impact global events, outstripping their expected reach and influence.

The inherent cyber vulnerabilities of these systems also highlight the need for comprehensive security measures. The effects of cyber operations can be seen in Ukraine and Gaza today. We haven't yet established what deterrence in cyber really is. We're still struggling to understand how cyber effects can best be marshaled alongside other, more traditional, effects of warfare.

The United States, China, Russia, and other major powers have begun rapidly expanding their own autonomous warfare capabilities, leading to strategic competition and security challenges, especially with the advancements being made by China. The dynamics of global competition, particularly in relation to drones and foreign military sales, present both opportunities and challenges in international relations and defense market shifts. It's important to note, also, the grave ethical concerns intrinsically linked to these technological advancements. While the United States and our allies and partners grapple with these challenges, it's unlikely the Chinese, Russians, Iranians, or other malignant actors are going to concern themselves with these questions when it comes to applying uncrewed and autonomous systems on the battlefield.

General (Ret) Frank McKenzie,
Executive Director, GNSI

# The Future and Ethics of Uncrewed and Autonomous Warfare
*8th Great Power Competition (GPC) Conference September 27-28, 2023*

## Introduction

On September 27-28, 2023, the Global and National Security Institute (GNSI) held the 8th Great Power Competition Conference titled "The Future and Ethics of Uncrewed and Autonomous Warfare" at the University of South Florida's Tampa campus. As a featured event of the 2nd GNSI Tampa Summit, the conference included three major panels: "Foreign Defense Partnership in a Global Competitive Market," "Ethical Use of Uncrewed Warfare," and "Future of Uncrewed Systems: The Benefits and Dangers of Advancing Technology." These panels brought together experts to discuss the evolving role of uncrewed and autonomous systems in warfare, their ethical implications, and the impact on global defense strategies, with a focus on the challenges and opportunities for major powers in this rapidly advancing field.

## Autonomous Warfare: A New Arena

**General (Ret) Frank McKenzie**'s opening remarks at the conference set the stage for discussion, as he provided a sobering overview of warfare's trajectory, asserting that "the use of uncrewed platforms and the applications of artificial intelligence and machine learning are going to dominate operations in space" and equally "on the face of the globe." This shift toward technology-intensive warfare, may not only redefine the essence of combat, but also the training and doctrine of the armed forces. While General McKenzie emphasized the increasing importance of autonomous warfare as a new method of combat, he cautioned us not to underestimate the likelihood of a resurgence in nuclear weaponry, specifically tactical ones. As he stated, "It's been nearly 80 years since a nuclear weapon was used against an enemy. I believe, again, we're much closer to that time occurring again, and it's one of the things that worries me the most as I look at what's going on in Ukraine." General McKenzie anticipates the battlefield will become increasingly populated with semi-autonomous and possibly fully autonomous systems; pointing toward a future where human decision-making is supplemented—or in some cases, supplanted—by algorithms and machine learning processes.

**Jaret Riddick** further examined the practical applications of new technologies, as well as artificial intelligence (AI) and the threats against United States (U.S.) national security, providing a multi-dimensional perspective into the ongoing evolution in military strategy.

Riddick observed that official Department of Defense (DOD) documents predict the ubiquity of crewed and autonomous systems on the battlefield. The idea that modern conflicts are now arenas for new technologies to be tested and observed has been substantiated by the recent utilization of such systems in conflicts like Ukraine, where Riddick noted, " the adoption of the sort of systems and technology that was not in frequent use before this conflict started." The lessons drawn from the Armenia-Azerbaijan conflict over Nagorno-Karabakh, are similarly telling. Riddick cited Alexander Kott's articles on the transformative role of drones in conflict, indicating a shift in warfare dynamics. Adoption of these technologies is not optional but a necessity to maintain strategic dominance, as Riddick emphasized, "It's clear now that you'll be left behind. And so, I think we see now moves to get out in front of this."

Echoing Riddick's concerns, **Jennifer McArdle** articulated a vision for human-machine teaming that extends beyond conventional applications, as vividly demonstrated by current events in Ukraine and concepts like a fighter pilot with a "loyal wingman." She stressed the diverse potential for such teaming, suggesting that as military reliance on these teams grows, trust will become increasingly vital. Her insights suggest a future where AI is not merely an adjunct to military power but a core asset that necessitates careful cultivation and strategic integration into national defense policy.

Similarly**, Dave Des Roches** emphasized the human aspect in the control and application of uncrewed systems by stating "the only limiting factor on the future of uncrewed systems are people." This notion suggests that

while technological advancements progress, the ultimate utilization, management, and oversight of these systems will be constrained or enabled by human operators and decision-makers. His repetition of this point reinforces the centrality of human roles in the evolution of warfare.

**Caitlin Lee** contextualized the application of uncrewed warfare in conflict by pointing to the rapid progression of drone technology. By looking back to the conflicts in Afghanistan and Iraq and citing the Pentagon's transition from reluctance to robust adoption of drone capabilities, she noted a significant redistribution of power not just among nations, but also from centralized command structures. Lee suggested a similar shift to autonomous systems that operate without human intervention could redefine strategic stability and operational warfare.

**Lieutenant General Greg Guillot** supported Lee's argument that uncrewed systems are becoming an inseparable part of warfare, emphasizing the integration marks a paradigm shift in how operations are conducted. He noted, "Today compared to 1999, we have the capability to quickly and seamlessly integrate uncrewed assets into all aspects of our operations." Guillot's focus on resourcing, testing, and fielding these systems speaks to an urgency to not only keep pace with technological advances but to leverage them for strategic advantage. He expressed a future-oriented vision, where U.S. Central Command (CENTCOM)'s groundwork will pave the way for incorporating "new technology and capabilities into future operations," underscoring the ongoing nature of this transformation.

**Matthew Mullarkey** pointed out that not all uses of autonomous technology are lethal or kinetic, hinting at a broader scope of applications in the pre-kinetic space, such as reconnaissance, logistics, and supply chain management. His observation broadens the discourse around autonomous warfare to include non-combat applications that are integral to military operations.

Considering Caitlin Lee and General Guillot's comments on the growing presence of uncrewed systems in military operations, **Stephanie Tompkins** highlighted the specifics of Defense Advanced Research Projects Agency's (DARPA) current work in a program called Urban Reconnaissance through Supervised Autonomy (URSA), which she described as a system designed to "distinguish friend from foe in

crowded urban scenarios." This, she elaborated, involves "autonomous systems working in concert with humans to sort of probe and push at crowds to help segregate behaviors," showcasing the dynamic interplay between technology and human judgment.

Lastly**, Laura Cressy** spoke about the collaborative potential of autonomous systems, noting their effectiveness when used by international partners and allies. She highlighted the critical role foreign military sales processes play in fostering operational alignment and responsible stewardship of technology. "The foreign military sales process gives us the opportunity to train with the operators, train with the maintainers," Cressy emphasized the U.S.'s commitment to ensuring partners are "effective stewards of the technology."

## Autonomous Warfare: A New Global Competitive Market

In discussing the security of autonomous systems, **Jaret Riddick** opened the discussion by emphasizing the shift toward collaborative innovation in defense technology. Riddick recognized the innovation ecosystem as a critical arena for collaboration with international partners, different from traditional foreign military sales. He saw potential in coalescing around technology adoption strategies, stating, "Innovation adoption now becomes a potential way for us to collaborate with international partners." Riddick's comments on non-traditional business partners in the defense space underscored a significant shift in how the DOD approaches risk.

Additionally, **Steve Roach** touched upon the challenges posed by the People's Republic of China's (PRC) involvement in the global supply chain of Unmanned Aerial Vehicle (UAV) products. He cited examples like the TikTok app controversy to illustrate the blurred lines between state and corporate entities in China, leading to concerns about allegiance and data security. His suggestions to ban certain PRC goods and conduct more investigations reflect a strategic approach to regain control over supply chains and maintain a competitive edge.

Building on Roach's comments, **Arman Sargolzaei** pointed out the cyber vulnerabilities intrinsic to autonomous systems. He argued that any disruption in the safe operation of these systems constitutes a cyber-attack. There's a tension

between the confidence in systems deemed "un-hackable" and the reality that even a slight delay in communication between systems, like a UAV, could have significant unsafe consequences. This distinction underscored the precarious nature of security claims and the necessity of accounting for even the most minor vulnerabilities that could lead to disproportionate consequences in the field.

Continuing Sargolzaei's remarks, **Laura Cressy** underscored the importance of secure technological environments in the realm of acquisitions by U.S. partners that could potentially compromise cooperation. The safeguarding of foreign partners is also paramount, as seen in efforts to ensure that "Taiwan systems, for instance, remain secure." Cressy firmly dispelled any notion of a "race to the bottom" in strategic competition, articulating a principled stance on foreign sales: "We're not going to approve a sale in a region or to a country just because our competitor is going to do it." Sales must align with and advance U.S. foreign policy and national security objectives, not merely counteract competitor actions.

**Arman Sargolzaei** furthered the conversation by emphasizing the necessity of comprehensive testing and verification as necessary to ensure these systems are safe and secure.

In addition to technical testing, Sargolzaei highlighted supply chain vulnerabilities, with a significant focus on the human factor, which remains the most unpredictable element in supply chain security. Even components that are labeled "made in the U.S." or manufactured domestically are not immune to risks of sabotage or manipulation. Such acknowledgment of supply chain integrity issues reflects the complexity of securing autonomous systems against a backdrop of global manufacturing and distribution networks. Is this correct:

## Artificial Intelligence: Its Benefits and Dangers

The transformative potential of artificial intelligence (AI) and machine learning (ML) to reshape the nature of warfare, modern military strategies, and operations was highlighted by several esteemed speakers who each brought their own unique perspectives on the subject. **General McKenzie** emphasized the ubiquity of machine learning, which will be pivotal for distilling crucial data from an overwhelming influx of information. He stressed the need for "applications

of artificial intelligence and machine learning" that are set to "dominate operations in space," pointing towards a future where decision-making time horizons are "greatly compressed," and where the speed and volume of incoming data will necessitate reliance on AI in warfare.

Further elaborating on the transformative impact of AI in the military realm, **Lieutenant General Guillot** highlighted that with AI and machine learning, there is the prospect of aircraft executing tasks autonomously, processing human commands, and even adapting independently to changing situations. Autonomous functioning, as exemplified by Task Force 59 systems, represents a significant shift towards a more self-sufficient and efficient form of warfare. Guillot underscored the ongoing transformation within CENTCOM, which is "in the process of transforming how we command and control," with AI and machine learning at the heart of this transformation. These advances facilitate operations that are "automatic and instantaneous," potentially eliminating the delays inherent in traditional communication channels.

The current policy dialogue, which focuses heavily on the dangers, hazards, and bias of AI, could potentially stifle innovation, Jaret Riddick cautioned. "We have to be very careful that we don't miss the opportunity for innovation and that we don't handcuff ourselves in terms of the technology that we want to have for the future warfighter."

**Stephanie Tompkins** addressed the challenges in threat perception in autonomous warfare by noting that the risk of an "unconscious bias towards everything looking like a threat," could be either mitigated or amplified by autonomous systems. Her suggestion of practical exercises to discern intent resonates with Dr. Sargolzaei's emphasis on thorough testing, highlighting the importance of understanding and managing the human-technology interface in security scenarios.

The potential of AI to revolutionize military operations was a key point for **Jennifer McArdle** who emphasized its role in enhancing decision-making and managing the deluge of information that commanders face. She noted that AI could function as an analytical collaborator, aiding in intelligence analysis and red teaming which is the process of using Tactics, Techniques, and Procedures (TTPs) to emulate a real-world threat with the goal of training and measuring within the command-and-control centers. The implication is that AI

not only automates certain tasks but also complements and amplifies human cognitive abilities. McArdle's optimism about AI bridging the digital divide reflects a broader vision where AI's impact extends beyond military applications to broader societal benefits.

**Caitlin Lee** focused on the rapid development of large language models and AI anticipating the emergence of truly autonomous drones capable of independent decision-making in combat, representing a major technological trend that would transform the battle space. However, **Daniel Strand** pointed to the "language of autonomy" as a significant concern and tackled public and academic apprehension concerning truly autonomous systems, especially the fear of "killer robots." He emphasized that complete autonomy, particularly in decision-making that involves taking human life, is not an imminent feature of any military branch. He acknowledged both the potential and the limitations of AI, underscoring the caution needed when deploying AI in open, uncontrolled environments. Conversations with DARPA officials affirmed this stance, mitigating fears that AI-operated weapon systems will operate without human oversight.

**Lieutenant General Alexus Grynkewich** contemplated a scenario of engaging with a non-human adversary capable of rapid decision-making. He advocated for AI's role in decision-making within enemy airspace, which would require minimal to no communication with a commander. The identification of targets with human input, enhanced by machine learning, was also presented as a key area where AI could come to our assistance. He stressed the importance of pairing these technological innovations with valid concepts of operation and a solid ethical framework.

Lastly, **John Pelleriti** addressed the potential_security challenges of integrating AI into military operations, while simultaneously recognizing the complexities DOD faces in achieving an integrated command structure, and the challenges posed by competitors like the RC. Currently the PRC "drastically outspends us" in autonomous systems, however, Pelleriti sees a unique opportunity for the U.S. in its potential to partner with private enterprises, leading to a strategic advantage.

## The Ethical Use of Uncrewed Warfare

In addition to discussing the technological and practical aspects of autonomous warfare, the conference delved into the ethical quandaries posed by the increased incorporation of artificial intelligence (AI) and autonomous systems into military operations. The discussions ranged from the integration of ethical principles into AI algorithms to the legal implications of autonomous warfare.

According to **Lieutenant General Greg Guillot,** the strategic benefits of uncrewed systems are clear. As they transcend human physiological limits, offering "unprecedented persistence over a target area," which was vividly demonstrated when an MQ-9 observed and tracked a suspicious uncrewed aerial vehicle (UAV), illustrating the agility of these systems in shifting from reconnaissance to actively countering threats. However, these advantages come with ethical considerations. CENTCOM's concern with the "irresponsible use of this technology" by adversaries who may not exhibit the same commitment to minimizing collateral damage or distinguishing between combatants and non-combatants. The proliferation of such one-way attack systems has necessitated the development of both kinetic and non-kinetic countermeasures to address these "very real ubiquitous threats."

**Caitlin Lee** stressed the need to contemplate the ethical implications of autonomous technology and its potential impact on international law and ethics. She identified the central challenge for the national security community as the integration of laws of armed conflict (LOAC) into the algorithms that will drive autonomous systems without eroding the ethical foundations of warfare. The potential for burdensome excessive legal constraints on AI to impact U.S. operational effectiveness is a concern for Lee. She advocated for a balance between ethical conduct and maintaining operational advantage, acknowledging that while adversaries may employ autonomous systems without such constraints, the U.S. seeks to approach this new era responsibly. While Lee's comments were mostly focused on U.S. laws, **Jonathan Horowitz** examined the impact of autonomous weapons systems (AWS) on international humanitarian law (IHL). When addressing threats to U.S. national security, Horowitz did not perceive tethered drones as challenging the normative structure of international

humanitarian law. However, with fully autonomous systems, there is a recognition that new challenges and potential gaps in the law will arise. He pointed to certain types of AWS that the International Committee of the Red Cross (ICRC) believes should be explicitly prohibited, even in the absence of explicit international prohibitions.

Horowitz acknowledged the tension between regulatory self-restraint and the fear that others may exploit a lack of regulation. Yet, he maintains that adherence to the law of armed conflict should not be compromised by concerns over competitive disadvantages. He contends that all states, regardless of their strategic preferences, must be bound by IHL. Horowitz outlined a clear distinction between tethered drones, which are under direct human control, and autonomous weapon systems (AWS) that can select and engage targets without human intervention. The ICRC perceives gaps in international law regarding AWS, advocating for states to pursue legal clarifications and potentially new laws. The ICRC's concern is particularly focused on systems designed to target humans, suggesting that ethical problems intensify when human agency is removed from the decision-making process in warfare.

For Horowitz, the central ethical issue is the "removal of human agency in an inherently human endeavor." He stressed the pressure point of this concern is most acute when AWS has the capability to take human life. This perspective aligns with sentiments expressed by various states, reflecting widespread discomfort with the notion of machines making life-and-death decisions.

Moving to the ethical use of autonomous systems, **Daniel Strand** highlighted the multi-faceted nature of drones, which incorporate a range of technologies and require significant human involvement. Addressing the notion of unilateral action, he pointed out that both American administrations and European allies have grappled with the moral justifications of using drones for counterterrorism outside of formal war zones, with sovereignty and the proper conduct of war at the heart of the debate. Strand also brought forward the psychological and moral impact on drone pilots, suggesting they may experience moral injury due to the intimate and prolonged nature of their engagement with targets. His observation that the American military has focused on professionalizing and instilling a sense of ethical

responsibility within the drone force reflects an ongoing effort to align technological capabilities with ethical warfare principles.

Bolstering Strand's and Horowitz's ethical concerns, **Steve Roach** stressed the importance of coaching the use of UAVs within a structured ethical framework, suggesting this is as crucial as the systems themselves. The uncertainty surrounding the U.S. supply of more advanced UAVs to Ukraine underscores the ethical and strategic dilemmas faced by the U.S. in such conflicts. Roach's reflections reveal the trepidation about escalating commitments through the provision of these advanced systems, resonating with a broader cautionary stance on the proliferation of autonomous weapons.

While several speakers stressed the importance of the ethical use of autonomous systems**, Stephanie Tompkins's** discourse highlighted the fine balance between technological advancement and ethical considerations. The future of autonomous warfare appears poised on the cusp of new frontiers, with DARPA firmly entrenched in guiding its trajectory. However, as Tompkins candidly admits, even a group of humans cannot always reach a consensus on what is right and wrong in the chaotic theater of war—implying even greater complexities when those decisions are left to autonomous systems.

The gap between emerging technologies and legislation was a point of concern for **Jaret Riddick**. He highlighted the risk of legislative bodies, often lacking in technical expertise, crafting policies that might inadvertently limit the United States' ability to exploit technological advancements. "Yes, legislation is behind," Riddick noted, "if we put things in place that handcuff us early, they'll be hard to fix later on."

Acknowledging Dr. Riddick's comments, **Lieutenant General Grynkewich** underscored the need for a preemptive approach to navigate ethical issues, emphasizing the importance of moral restraint as the foundation for the approaches to using autonomous weapons. He reiterated the legal and ethical constraints inherent in military objectives, specifically the principle of distinction in the law of war. He also highlighted low-cost systems, such as swarms of sensors, could provide higher fidelity information without risking either workforces or sophisticated equipment.

In addressing the growth of regulations and laws on the use of unmanned warfare, such as drones, **Major General (Retired) Charles Dunlap** emphasized worries that more procedures could excessively burden commanders, possibly hindering their capacity to carry out missions effectively. His observations demonstrate a detailed grasp of the intricate and changing aspects of contemporary warfare. He warned against creating a bureaucracy that imposes additional processes on commanders who may need to act swiftly. He raised concerns that current plans do not sufficiently consider the impact of AI, especially generative AI, and its capability for rapid information generation.

## The Issue of Trust

In addressing the issue of trust in artificial intelligence (AI) within military contexts, **Paul Lushenko** revealed a concerted effort to understand trust within the context of large-scale ground combat operations. He emphasized the crucial role of soldiers in the "experimentation, the testing, the fielding of capability," indicating that the human component is integral to the operationalization of AI in military contexts. Lushenko's definition of trust as a willingness to be vulnerable to a capability, predicated on shared expectations and experiences, underscores the multifaceted nature of trust, which is not merely a product of technology's reliability but also of its integration into the fabric of military culture and values.

His exploration of trust in AI pointed to a gap in understanding "what features of a technology shape soldiers', especially soldiers', trust in these capabilities and adoption thereof." **Dave Des Roches** noted that trust could be enhanced through time, familiarity, established expertise, and rapport. These factors, which build a track record of reliability, are identified as valuable commodities in the landscape of modern warfare. In his analysis of warfare dynamics, Des Roches acknowledged that despite significant improvements in sensors, AI, and platforms, the fundamental nature of conflict remains unchanged since the time of the Roman legions—it is still a human endeavor. This perspective serves as a reminder that while the tools of war evolve, the human element remains at its core.

Regarding trends and technological advancements, Des Roches pointed to swarms and steerable hypersonic as the technologies to watch. Swarms, with their potential for decentralized operation and massed, coordinated action, and hypersonic, particularly those that are not just fast but also maneuverable, represent strategic advancements that could redefine engagement and deterrence paradigms.

Des Roches underscored this by addressing the prevention of false positives—a crucial safeguard in military operations that depend on the accuracy and reliability of the systems employed. His emphasis on the emotional component of trust reflects an understanding that reliance on technology, especially in life-and-death scenarios, involves more than just rational calculations—it taps into deeper psychological aspects of human-machine interaction.

In parallel to Lushenko and Roches 'comments on the issue of trust, **Rogers Kangas** argued for a critical examination of how these systems could be integrated with human operators underscoring the unease and uncertainty accompanying the handover of lethal decision-making from human to machine. "f [H]ow do we rely on these as an integrated system with humans... [is]going to be some challenging."

Finally, **Michael Kreuzer** concluded the discussion by pointing out an intriguing observation about the varying levels of trust commanders place in AI, which seems inversely proportional to their experience with the technology: "We noted that some commanders actually, the less experience they have with AI in some cases, the more artificial trust they're going to have with them." The trust in artificial intelligence, which Kreuzer referred to as "artificial trust,", poses significant implications for the deployment of AI systems on the battlefield, as inexperienced users may either over-rely on or misuse AI capabilities due to misplaced confidence.

## Threats Against the U.S. National Security

The conference brought to light these evolving dynamics through the insights of key military leaders and experts, particularly focusing on the challenges posed by major global powers and the impact of emerging technologies on strategic superiority. As the landscape of international relations and military capabilities continues to transform, the United States faces the critical task of reevaluating and responding to these multifaceted threats to ensure its security and maintain its strategic position on the global stage. In this context, **General McKenzie** highlighted that the "capability advantage" the United States once enjoyed is eroding, with China and Russia, particularly China,

closing the gap. This is manifested in China's focus on hindering the United States' ability to deploy and command forces effectively. McKenzie did not overlook smaller, yet significant, actors like Iran, whose investment in missile and drone technology represents a substantial threat to regional stability.

General McKenzie articulated the United States' dual challenges: a "decades-long" struggle with China and an "immediate challenge" from Russia. These long-term and immediate concerns are part of the broader discourse on drones, uncrewed systems, and autonomous systems—the "meat and potatoes of this conference." General McKenzie's remarks did not shy away from the domestic implications of autonomous warfare. He posited that "in any kind of a future war, our homeland here in the United States, we're going to be attacked in ways that we've never been attacked before." This projection was not confined to the physical realm but extended to the cyber domain, with McKenzie asserting that future conflicts would have "global effects," encompassing the "silicon pathways of the vast and infinite web" and extending to "cis-lunar space." Such statements highlight the blurring lines between conventional battlefields and new fronts in cyberspace and outer space.

What was once the comforting vastness of oceans safeguarding the United States is now, in McKenzie's view, analogous to "little more than river barriers," due largely to the "ranges and speed of modern missiles." This metaphor starkly illustrates the reduced protective buffer for the nation, as missile technology, including hypersonic capabilities, shortens the distance between adversaries. McKenzie further emphasized the nation's vulnerability through the lens of cyberinfrastructure, describing it as "fragile" and alarmingly open to exploitation, especially by actors like China, with their significant advancements in multiple disruptive technologies.

Navigating this "new and complex environment" will involve grappling with the accelerated demand for information and the increased difficulty of its collection in likely combat conditions. General McKenzie touched upon an immutable truth of warfare—that disruption is often easier than creation. This idea, when applied to cyber warfare, becomes a critical point of consideration, particularly when decisions must be made at "machine speed."

The recognition of space and cyber as domains of conflict resonated throughout McKenzie's presentation, framing them as "relatively new domains of warfare" that have evolved from uncontested spaces to battlegrounds. The acknowledgment of uncrewed aerial systems overflying bases in the central command region further underlines the transition towards an era where such threats are already a reality.

**Jaret Riddick** built upon General McKenzie's discussion regarding the rapid advancement in autonomous warfare by US adversaries, pointing out the numerical advantages countries like China hold. However, he advocated for leveraging America's qualitative edge, stating, "We are in a position where the quantity on the other side is challenging, but we have to really double down in quality."

Continuing the dialogue regarding China's swift progress in autonomous warfare, **Caitlin Lee** underscored the heightened strategic rivalry with China, characterizing it as the most significant threat to U.S. national security. This competition shapes the discourse on the future of drone warfare, leading to a security dilemma where advancements by one nation drive the other to react similarly. The worry is that this competition may evolve from current uses to more deadly applications, potentially triggering an arms race in autonomous weapons.

Similarly, **Steven Luxion** conveyed a sense of urgency, stating that "inherently we are behind." The U.S. government's conscious decision to avoid Chinese products for security reasons is valid, but there is an emerging gap because domestic industry has not fully risen to meet the demand. : "So we have some serious catching up to do as we move forward and we got to overcome that challenge because if [the] industry's not there, that's a national security risk that we have to fix," he stated.

**Matthew Mullarkey** expanded on the vulnerabilities created by ubiquitous autonomous systems across multiple industries, from energy to medicine and package delivery. The omnipresence of these systems signifies a widespread impact on society and, by extension, the security landscape. His repetition of the vulnerability of networks underscores the strategic importance of cyber-hardening measures.

Cressy firmly dispelled any notion of a "race to the bottom" in strategic competition, articulating a principled stance on foreign sales: "We're not going to approve a sale in a region or to a country just because our competitor is going to do it." Sales must align with and advance U.S. foreign policy and national security objectives, not merely counteract competitor actions.

**Stephanie Tompkins** also remarked that threats against U.S. national security coming from autonomous systems growing," drawing a parallel with DARPA's inception, which was in response to "the launch of the Sputnik satellite." She reminded the audience that the "DARPA approach to that mission has been to always be at the bleeding edge" to preempt technological surprises from adversaries.

While other speakers focused on great power competition in autonomous warfare and related technological vulnerabilities, **Stipe Skelin** highlighted the changing dynamics of global competition, particularly in relation to drones and foreign military sales (FMS) systems. These developments offer both opportunities and challenges for international interactions. Skelin pointed out China's transition from a major importer to a confident exporter of military equipment, a change that reflects broader shifts in the global defense market and the impact of emerging technologies on international power structures.

Addressing threats to U.S. national security, Skelin emphasized the dilemma posed by the restrictive nature of FMS, which is bound by U.S. regulations, including human rights considerations. These constraints are not shared by competitors like China, Iran, and Russia. He suggested that these nations operate with pragmatism and patience, steadily expanding their influence. Skelin proposed that the U.S. must remain vigilant and proactive, viewing allies and partners not just as market competitors but also as potential collaborators in security initiatives to counter the influence of these rivals.

Furthermore, Skelin highlighted a critical technological issue: the incompatibility of Chinese, Iranian, or Russian systems with those provided by the U.S. This incompatibility presents a strategic challenge, as partners who acquire military equipment from these nations might face difficulties integrating with U.S.-led systems, potentially isolating them from U.S. support and operations.

**Jennifer McArdle** echoed these sentiments, highlighting the strategic competition with China, particularly in research and development (R&D) spending and talent acquisition through programs like China's Thousand Talents Program. McArdle suggested that an immigration policy could be a strategic tool to counter such competitive strategies, underscoring the need for strategic policy thinking in the face of rapid technological advancement.

## Strategies for the Future of Uncrewed Systems

Uncrewed and autonomous warfare marks a significant transformation in military tactics and strategy, utilizing advanced technology to improve combat effectiveness while minimizing human risk. A key focus among the speakers was for the United States to develop a thorough blueprint for navigating the future of autonomous warfare. Advocating for an approach that not only involves technological development but strategic, ethical, and legal considerations. Ensuring the U.S. remains at the forefront of an evolving battlefield while adhering to its principles and international norms.

**General McKenzie** set the stage with a stark reminder of the need for recognition and preparation in the face of relentless preparation by potential adversaries. He warned that other nations are "relentlessly preparing for this war" and that such preparations are directly "targeting us." This call to action served as a stark reminder of the need for the United States to both recognize and adapt to the "shape and contour of what the next war could be." The transition towards autonomous warfare systems seems inevitable, but it is fraught with challenges that must be met with rigorous training, robust ethical frameworks, and a forward-thinking defense posture that can safeguard national security while adapting to the changing nature of global conflict.

In the labyrinth of military technology and ethics, General McKenzie's perspective serves as a warning to the decision-makers. His discourse at the conference was not merely a reflection on the potential of autonomous warfare but a clarion call to recognize and navigate the pressing realities that come with such advancement.

General McKenzie firmly placed information at the core of future warfare, stating, "The next war is going to be driven by information, collecting it, processing it, using it efficiently and denying an adversary's ability to do the same

is going to be the central calculus of that war." This is not just theoretical; the ubiquity of uncrewed platforms in the central command region and the recent conflicts, such as in Ukraine, is a testament to a growing trend that McKenzie anticipates will only intensify. The integration of uncrewed systems "in tandem with manned platforms," particularly in the Air Force, suggests a hybrid future where human and machine-operated systems operate in concert.

In the realm of artificial intelligence, **Jonathan Horowitz** advocated for nuanced discussions on the use of AWS, moving beyond binary debates to consider how these systems should be used based on their capabilities and the contexts in which they are deployed. He also suggested that limitations might be necessary—for example, restricting the use of fragile autonomous systems with AI in complex urban environments.

Regarding the issue of trust, **Paul Lushenko** proposed studying soldier attitudes toward these systems to discern the variables that influence their trust and, consequently, their adoption of the technology. His recognition of trust as "complex and multi-dimensional" indicates that it varies by situation and individual personality, making the study of trust in military AI applications a challenging yet essential endeavor. To advance this understanding, Lushenko suggested a research agenda that investigates soldiers' attitudes toward AI from the very beginning of their military careers, including at military academies. He posited that a quantitative research methodology could elucidate the factors that shape trust, which would have implications for how AI technologies are introduced and integrated into military use. The concept of "digital natives" was also touched upon, with Lushenko postulating whether younger soldiers, presumed to be more technologically adept, might inherently place more trust in AI systems simply due to their upbringing in a digital world.

**Steven Luxion** shifted the focus to the regulatory challenges, highlighting a leadership problem within regulatory bodies such as the Federal Aviation Administration (FAA). The risk-averse nature of the FAA, he suggested, hinders the agility required in the modern age: "The bureaucracy is heavy and it's very, very difficult for the FAA currently to move, it's a risk-averse organization anyway." The challenge of certifying autonomy, especially in systems that are primarily software-based, is exacerbated by outdated certification processes that struggle to keep pace with technological advancements. Luxion's comments about the talent pool and regulatory mindset present an opportunity for innovation in governance. He called for harnessing the "immense talent out there" to educate and shift the mindset of regulatory leaders. The key to future safety, according to Luxion, may lie in redefining safety protocols to align with new technological realities.

Public trust emerges as a critical theme in Luxion's discussion. The FAA's cautious approach, he suggests, stems from uncertainty about societal acceptance of autonomous systems: "What's holding up the FAA and the leadership and general counsel is they don't know where our citizens sit in the nation, their comfort and trust in these systems." This overregulation as a safeguard against potential public backlash underlines the need for a more informed and engaged dialogue with the public to gauge comfort levels and educate on the benefits and safeguards of autonomous systems.

**Steve Roach** suggested that a more critical analysis should be given to "policy changes" in targeting enemies via UAVs. He referenced recent policy shifts that impact how the U.S. defends itself and its allies against terrorism, hinting at the implications of such policies on both combatant and civilian populations. The estimated number of civilian casualties from UAV strikes he mentioned points to a substantial ethical issue, raising the question of proportionality and the necessity of refining targeting protocols to minimize such collateral damage. Roach argued for market-based strategies combined with governmental action to address dependency on foreign supply chains, particularly those from the PRC. He critiqued the Trump administration's policy changes regarding drone strike thresholds, which he believed led to increased civilian casualties, questioning the morality and acceptability of such a stance. In proposing solutions, Roach underscored the importance of building partnerships and coalitions to prevent the adverse effects of open competition and to promote a form of integrated deterrence.

Furthermore, **Lieutenant General Grynkewich** acknowledged the increased speed of warfare at both tactical and operational levels and the extended logic of autonomy from a fighter aviation perspective to various military concepts. He stressed that uncrewed and fully autonomous systems offer opportunities to scale up and mass effects

without risking human lives. He also highlighted the need for the military to be capable of rapidly producing and procuring systems capable of executing high-end full-scale operations.

Grynkewich addressed the constraints that must be placed on autonomous systems and the importance of human guidance in engagement scenarios. He argued for the need for autonomous systems to be auditable and transparent in their decision-making processes that could provide ethical principles to guide AI development.

Echoing General Grynkewich's suggestions, **Matthew Mullarkey** emphasized that the pace at which these innovations are advancing necessitates a robust security posture, especially for networks that will integrate drones and autonomous vehicle systems. He posited that "every network is at risk," highlighting the need for hardened networks against potential threats.

Lastly, **Major General (Ret) Charles Dunlap** emphasized the changing nature of military operations, particularly in the context of developments observed in Ukraine. He noted that the era of large command posts is effectively over, as their significant signatures make them vulnerable. This shift has led to a more distributed approach to operations. Dunlap highlighted the need for specialized expertise in modern warfare. He stated that future commanders will require experts in artificial intelligence and information operations. These specialists would complement the traditional roles within a command unit, like intelligence officers and civil engineers. Dunlap suggested that existing personnel could be trained to meet new requirements or to gain additional expertise as needed.

A crucial point raised by Dunlap was the importance of countering enemy narratives. He believes that while civilian harm mitigation processes are vital, they could be undermined if the enemy successfully creates a convincing narrative. This perspective underscores the growing significance of information warfare and the need for competence in managing and countering narratives in modern conflict scenarios.

---

## The BIG 3 Takeaways

1) **As warfare evolves with autonomous and uncrewed technology, there's a pressing need to balance these advancements with ethical considerations. This involves grappling with the complexities of AI and machine learning in combat, ensuring that technological strides don't outpace the legal and moral frameworks necessary for their responsible use.**

2) **The summit brought to light the strategic challenges posed by autonomous warfare. It's crucial to proactively address these emerging threats, emphasizing the need for a robust defense against the vulnerabilities of these technologies, including supply chain risks and cyber threats. This requires a forward-thinking approach to maintain global security in the face of rapid technological change.**

3) **A key consensus was the need for a holistic strategy that goes beyond technological development. This includes fostering international cooperation to establish norms and frameworks for the ethical use of autonomous systems, ensuring that their integration into military operations adheres to ethical warfare standards and global security concerns. This approach underscores the importance of a unified, responsible stance on the future of warfare technology.**

**Arman Mahmoudian**, PhD Candidate
Armanm@usf.edu

**8ᵗʰ Great Power Competition Conference – The Future and Ethics of Uncrewed and Autonomous Warfare**
September 27-28ᵗʰ, 2023

**Day 1**
September 27, 2023 (Conference Video Day 1 available at GNSI YouTube page: GNSI Tampa Summit 2: Day 1 – The Future and Ethics of Uncrewed and Autonomous Warfare – https://www.youtube.com/watch?v=bjA5v5HUosI

*Speakers*
Dr. Eric Eisenberg, Senior VP, University-Community Partnerships, University of South Florida
General (Ret) Frank McKenzie, Executive Director, GNSI
Lieutenant General Greg Guillot, Deputy Commander, United States Central Command
Major General (Ret) Charles Dunlap, Jr., Executive Director, Center on Law, Ethics and National Security, Duke University

*Panel 1: Foreign Defense Partnerships in a Global Competitive Market*
Moderator: David Des Roches, Associate Professor, Near East South Asia (NESA) Center for Strategic Studies
Brigadier General (Ret) John Pelleriti
Laura Cressey, Director, Office of Regional Security and Arms Transfer, U.S. State Department
Lieutenant Commander, Stipe Skelin, Croatian Navy, currently assigned to Combined Strategic Analysis Group, United States Central Command
Dr. Steven Roach, Professor of International Relations, University of South Florida

*Round Table: Ethical Use of Uncrewed Warfare*
Facilitator: Lieutenant Colonel Paul Lushenko, PhD, Director of Special Operations. U.S. Army War College
Dr. Daniel Strand, Assistant Professor of Ethics, U.S. Air Force War College
Jonathon Horowitz, Legal Advisor, International Committee for the Red Cross, Regional Delegation for the United States and Canada
Caitlin Lee, Director, Acquisition and Technology Policy Program, RAND Corporation
Lieutenant Colonel Michael Kreuzer, PhD, Director of Operations Support Squadron, Joint Base Langley-Eustis, Virginia

**Day 2**
September 28, 2023 (Conference Video Day 2 available at GNSI YouTube page: GNSI Tampa Summit 2: Day 2 - The Future and Ethics of Uncrewed and Autonomous Warfare - https://www.youtube.com/watch?v=ljJynGmu0eE

*Speakers*
Dr. Roger Kangas, Academic Dean, Near East South Asia (NESA) Center for Strategic Studies
Dr. Stefanie Tompkins, Director, Defense Advanced Research Project Agency (DARPA)
Lieutenant General Alexus Grynkewich, Commander Ninth Air Force (Air Forces Central)

*Panel 2: Future of Uncrewed Systems, The Benefits and Dangers of Advancing Technology*
Moderator: Dr. Arman Sargolzaei, Director, Resilient, Autonomous, Networked Control System (RANCS) Research Group, Assistant Professor University of South Florida
Colonel (Ret) Steve Luxion, Executive Director, Alliance for System Safety of UAS Through Research Excellence (ASSURE)
Dr. Jaret Riddick, Senior Fellow, Georgetown University's Center for Security and Emerging Technology (CSET)
Dr. Jennifer McArdle, Adjunct Senior Fellow, Defense Program, Center for New American Security (CNAS)

*Introduction to Recap of Four Breakout Sessions*
*BREAKOUT SESSION #1: AI Ethics in Lethal Autonomy*
Recap with Lieutenant Colonel (Dr.) Paul Lushenko, and Lieutenant Colonel Michael Kreuzer
*BREAKOUT SESSION #2: Future of Uncrewed Systems*
Recap with Dave Des Roches
*BREAKOUT SESSION #3: INDUSTRY USE AND ADVANCEMENT OF UAVs*
Recap with Matthew Mullarkey
*BREAKOUT SESSION #4: SECURITY OF AUTONOMOUS SYSTEMS*
Recap with Dr. Arman Sargolzaei

# NOTES

**UNIVERSITY** of
**SOUTH FLORIDA**
**Global and National Security Institute**

Operating at the boundary of
## TECHNOLOGY AND POLICY

**UNIVERSITY** of
# SOUTH FLORIDA
## Global and National Security Institute

GNSInstitute@usf.edu
usf.edu/gnsi

in
@company/usfgnsi

𝕏
@USF_GNSI

▶ YouTube
@USF_GNSI