2025

Global Challenges in Public Safety & Defense

Navigating the Contemporary Strategic Environment

A Strategic Analysis by

KNOWUS

Executive Summary

The global Public Safety and Defense sectors are confronting a period of profound and systemic disequilibrium. The contemporary strategic environment is no longer defined by discrete, predictable threats but by the convergence of powerful global megatrends that are generating more frequent, intense, and cascading crises. The confluence of renewed great power competition, accelerating technological disruption, the escalating impacts of climate change, and deep-seated institutional decay has created a uniquely contested and volatile landscape. This environment is characterized by a looming imbalance between the scale of emerging challenges and the capacity of existing institutions, doctrines, and resources to respond effectively. From the return of industrial-scale warfare in Europe to the weaponization of information targeting domestic populations, and from the ethical dilemmas of artificial intelligence to a deepening crisis in human capital, the challenges are interconnected and mutually reinforcing. Navigating this new era requires a fundamental rethinking of traditional concepts of security, a "whole-of-society" approach to resilience, and a renewed commitment to the institutional legitimacy that underpins both national defense and public safety.

Michael Dalsgaard
Founder
KNOWUS

I. Introduction: A New Era of Converging Crises

Defining the Sectors

The concepts of Public Safety and Defense, while distinct, are increasingly intertwined in a complex global security ecosystem. The Defense sector traditionally centers on safeguarding countries through military operations, strategic planning, intelligence, and maintaining national stability against external threats. Public Safety, in its broadest sense, involves protecting the public from crimes, disasters, and other dangers, a responsibility carried out by a wide array of government and civil organizations. This includes not only law enforcement and emergency response but also judicial systems, corrections, border security, and public health organizations. This comprehensive definition is essential for understanding the contemporary threat landscape, where the lines between foreign aggression and domestic security are increasingly blurred. An adversary's cyberattack on a nation's power grid, for instance, is simultaneously an act of foreign aggression and a catastrophic public safety emergency.

The Central Thesis: A System of Interlocking Megatrends

The current strategic environment is being reshaped not by singular events but by the confluence of several global megatrends - large-scale, long-term macroeconomic and geostrategic forces that are altering the world.[1] The central challenge facing Public Safety and Defense is that these trends are not acting in isolation; they are interacting, creating feedback loops that amplify their disruptive effects and produce cascading, often unpredictable, crises. This dynamic is creating what the U.S. National Intelligence Council describes as a "looming disequilibrium between existing and future challenges and the ability of institutions and systems to respond".[1] The primary megatrends driving this instability are geopolitical fragmentation, disruptive technological change, climate change and resource scarcity, and profound demographic and socio-economic shifts.[2] The interaction of these forces is straining the resilience of communities, states, and the international system, often exceeding the capacity of existing models and institutions. The result is a more contested world at every level: communities are fractured, states are struggling to meet public expectations, and the international system is more competitive and prone to conflict.[1] The following table provides a strategic overview of these megatrends and their primary impacts across the Defense and Public Safety sectors, establishing a framework for the detailed analysis that follows.

Table 1: Strategic Overview of Megatrends

Megatrend	Description	Primary Impact on Defense	Primary Impact on Public Safety
Geopolitical Fragmentation	A shift from a unipolar or bipolar world to a more contested, multi-polar environment with rising great power competition and a fracturing of global norms and institutions.	Increased defense spending and arms races; heightened risk of state-on-state conflict; supply chain vulnerability; rise of hybrid warfare and gray zone conflict.	Increased risk of state-sponsored disinformation targeting domestic populations; spillover effects of foreign conflicts (refugee flows, terrorism); strain on border security.
Technological Disruption	The exponentially rapid development and diffusion of new technologies, particularly AI, autonomy, cyber capabilities, and biotechnology.	Transformation of the battlefield (unmanned systems, AI-enabled command); race for technological superiority; new domains of warfare (cyber, space); ethical dilemmas of autonomous weapons.	Proliferation of advanced cybercrime targeting critical infrastructure; challenges of digital forensics; ethical issues of predictive policing and surveillance; need for costly technology upgrades.

Climate Change & Resource Scarcity	Rising global temperatures, more frequent and severe extreme weather events, sea-level rise, and resulting scarcity of critical resources like water and food.	A "threat multiplier" that accelerates instability and conflict; direct threats to coastal military installations; increased demand for humanitarian assistance and disaster relief (HADR) missions.	Overwhelmed emergency response systems; infrastructure damage; resource competition leading to local conflict and crime; mass migration and displacement.
Demographic & Socio-Economic Shifts	Aging populations in developed nations, youth bulges in others, accelerating urbanization, and growing economic inequality and social polarization.	Shrinking recruitment pools in the West; budget pressures as healthcare costs rise; instability in regions with large, unemployed youth populations.	Link between economic distress and crime rates; challenges of policing megacities; recruitment and retention crisis in law enforcement; erosion of public trust in institutions.

**Data synthesized from National Intelligence Council and PwC analyses.*[1,2]*

II. The Fracturing Global Order: Geopolitical Instability and the Evolving Character of Conflict

The post-Cold War era of relative stability has given way to a period of intense and complex geopolitical competition. This fracturing of the global order is manifesting in a return to state-on-state rivalry, the rise of ambiguous forms of conflict that blur the line between war and peace, and a shifting landscape of transnational threats like terrorism.

The Resurgence of Great Power Competition

The most significant geopolitical shift is the return to an era of strategic competition between major powers, fundamentally altering national security priorities and resource allocation. Global defense spending reached a record $2.443 trillion in 2023, the ninth consecutive year of increases, fueled primarily by the war in Ukraine and escalating tensions in the Middle East and the Indo-Pacific.[3] Russia's full-scale invasion of Ukraine in 2022 served as a catalyst, prompting a widespread re-evaluation of defense postures across Europe. Germany, for example, announced a landmark injection of $108.32 billion into its defense budget, while NATO allies have been forced to rapidly increase spending to replenish their own arsenals after providing extensive military aid to Ukraine.[3]

This spending surge reflects a renewed focus on high-intensity, conventional warfare, a domain that had been de-emphasized during decades of counter-insurgency operations. This pivot back to industrial-scale conflict has exposed a critical vulnerability: the fragility of globalized defense supply chains. Decades of optimizing for efficiency have created extensive and complex supply networks that are now strategic liabilities. The conflict in Ukraine has revealed significant delays in procuring military equipment and ammunition, stemming from surging demand and disrupted production capabilities.[4] This vulnerability is exacerbated by geographic dependencies, such as the heavy reliance on Taiwan for advanced semiconductor production and China for rare earth minerals, both of which are essential for modern defense systems.[4] A disruption in these key regions could ripple through global supply chains, crippling both defense and civilian industries and creating severe inflationary pressures.

This reality has created a significant strategic challenge for defense planners. They are being pulled in two opposite directions at once. On one hand, the war in Ukraine demonstrates the enduring relevance of industrial-age, attrition-based warfare, which demands massive stockpiles of munitions, robust logistical chains, and a resilient industrial base capable of producing at scale. On the other hand, adversaries are increasingly employing information-age, ambiguity-based hybrid warfare, which operates below the threshold of conventional conflict and requires entirely different capabilities. These two modes of conflict demand fundamentally different mindsets, training, and resource allocations. One requires steel, fuel, and industrial capacity; the other requires intelligence analysts, cyber operators, and a well-informed, resilient populace. A nation that invests heavily in

tanks and artillery to deter a conventional invasion may find its political will to use that army eroded from within by a sustained disinformation campaign. Conversely, a nation focused solely on hybrid defense may lack the industrial depth to sustain a high-intensity conflict should deterrence fail. This creates a critical and difficult trade-off, a "strategic squeeze" that defines the modern defense planning environment.

The Gray Zone: Countering Hybrid Warfare and Disinformation

In parallel with the return of conventional threats, the space between peace and war - often called the "gray zone" - has become a primary arena for state competition. Adversaries are increasingly employing hybrid warfare, a military strategy that blends conventional and irregular tactics with non-military instruments of power.[5] These methods include cyberattacks, economic coercion, political subversion, the use of proxy forces, and, critically, disinformation campaigns. State actors like Russia have integrated these tools to achieve strategic objectives gradually, seeking to avoid clear attribution and complicate a decisive response from Western nations and alliances like NATO.[5]

The explicit goal of these campaigns is to exploit and exacerbate a target nation's existing societal vulnerabilities, such as political polarization, economic inequality, or ethnic tensions. By spreading disinformation and propaganda through social media and other channels, these actors aim to undermine public trust in democratic institutions, sow discord, and weaken societal cohesion, thereby achieving the "inner decay" of an opponent without a direct military confrontation.[6] This represents a fundamental shift in the nature of conflict, where the "battlespace" is no longer a physical location but the human consciousness and information environment of the target society.

This dynamic effectively collapses the traditional distinction between foreign and domestic threats. The tools of hybrid warfare directly target the domestic sphere, making public safety a core component of national security. A state-sponsored cyberattack on a local water utility or a disinformation campaign aimed at disrupting an election is not merely a crime or a political issue; it is an act of foreign aggression playing out within a nation's borders. This reality places domestic law enforcement, intelligence agencies, and critical infrastructure operators on the front lines of geopolitical conflict, requiring a level of integration and coordination between national security and local public safety agencies that most countries are not currently structured to handle. Countering these threats, therefore, requires more than just a military response; it demands a "whole-of-society" approach that builds national resilience through robust security organizations, a strong security culture, and clear crisis management plans that span public and private sectors.[7]

The Shifting Epicenter of Terrorism

While great power competition dominates headlines, the threat of terrorism continues to evolve. According to the 2024 Global Terrorism Index, the global impact of terrorism is worsening, even as its geographic focus shifts. In 2023, deaths from terrorism increased by 22% to 8,352, the highest level since 2017. This occurred even as the total number of terrorist incidents fell by 22%, indicating that attacks have become significantly more lethal.[8]

The most profound trend is the geographic shift of terrorism's epicenter. The Central Sahel region of sub-Saharan Africa has now conclusively overtaken the Middle East, accounting for over half of all deaths from terrorism globally.[8] Countries like Burkina Faso, Mali, and Niger have experienced a catastrophic deterioration in security, with groups affiliated with Islamic State (IS) and Al-Qaeda, such as Jamaat Nusrat Al-Islam wal Muslimeen (JNIM), being the most active and deadly terrorist organizations.[8] This shift highlights a powerful and persistent insight: the inextricable link between conflict and terrorism. Over 90% of terrorist attacks and 98% of terrorism deaths in 2023 occurred in countries already experiencing violent conflict, underscoring how

state failure, political instability, and ongoing warfare create the ideal conditions for extremist groups to emerge, recruit, and operate.[8]

III. The Double-Edged Sword: Technological Disruption in Security and Defense

The exponentially rapid development and diffusion of new technologies is arguably the most transformative force shaping the security environment. From cyberspace to artificial intelligence, these technologies offer unprecedented capabilities for both defenders and adversaries, creating a complex landscape of opportunity, risk, and profound ethical challenges.

The Digital Battlefield and Homeland

Cyberspace has become a primary domain for both conflict and crime, posing a strategic risk to national security, economic prosperity, and public safety. Malicious actors, including sophisticated nation-states and transnational criminal organizations, are relentlessly targeting critical infrastructure sectors such as energy, water, healthcare, and finance. Their objectives range from espionage and intellectual property theft to laying the groundwork for future disruptive attacks that could have devastating physical consequences. The increasing convergence of informational technology (IT) and operational technology (OT) systems - the digital controls for physical infrastructure - has dramatically expanded the attack surface, making these vital systems more vulnerable than ever. Recognizing this threat, governments have established new entities to counter it, such as the U.S. Disruptive Technology Strike Force, which aims to prevent adversaries like China, Russia, and Iran from illegally acquiring sensitive technologies that could be used to enhance their military and surveillance capabilities.[9]

Simultaneously, technology is transforming the character of conventional warfare. The modern battlefield is witnessing a proliferation of cheaper, more lethal unmanned systems - in the air, on land, and at sea - that are changing operational calculus. An explosion of open-source intelligence, from commercial satellite imagery to social media analysis, is creating unprecedented transparency, making it harder for forces to achieve surprise. The integration of artificial intelligence, quantum computing, and space-based sensors promises to accelerate decision-making and create new military advantages, but also generates a "ravenous need for data storage and cloud computing".[10]

This technological race is creating a widening asymmetry that favors attackers over defenders in the cyber domain. The proliferation of sophisticated, commercially available tools, supercharged by advances like generative AI that can create highly convincing phishing attacks at scale, has dramatically lowered the barrier to entry for malicious actors. Meanwhile, defenders, especially in the public sector, are often hampered by underfunding, a shortage of skilled personnel, and the need to protect vast and often outdated legacy systems. This fundamental imbalance - where defenders must protect every potential vulnerability while an attacker need only find one - is becoming unsustainable. It suggests that a strategic shift is necessary, moving from a primary focus on prevention (building higher digital walls) to an emphasis on resilience: the ability to withstand an attack, continue to operate in a degraded environment, and recover quickly.

The AI Revolution: Opportunities, Risks, and Ethical Frontiers

Artificial Intelligence (AI) stands at the center of the technological revolution, presenting a dual-use dilemma on a global scale. The same core technologies - machine learning, data analytics, and autonomous systems - are simultaneously transforming military warfare and domestic policing, but the ethical and legal frameworks governing their use are developing in dangerously divergent and uncoordinated ways.

In the military domain, the prospect of Lethal Autonomous Weapon Systems (LAWS) - weapons that can independently search for, identify, and kill human targets without direct human control - raises profound ethical

and legal questions about ceding life-and-death decisions to machines.[11] International bodies like the International Committee of the Red Cross (ICRC) have highlighted the immense challenge of ensuring these systems comply with the core principles of International Humanitarian Law (IHL), such as distinction (differentiating combatants from civilians), proportionality (ensuring collateral damage is not excessive), and precaution (taking all feasible measures to avoid civilian harm).[11] A critical concern is the "accountability gap": if an autonomous system makes an unpredictable or erroneous decision that leads to a war crime, it is unclear who can be held legally responsible—the commander who deployed it, the programmer who coded it, or the manufacturer who built it. The central debate revolves around the necessity of maintaining "meaningful human control" over the use of force.[11]

In the realm of public safety, AI is being deployed in the form of "predictive policing" systems, which use historical crime data to forecast where and when future crimes are likely to occur, or to identify individuals at high risk of offending or being victimized.[12] Proponents argue these tools can optimize the allocation of scarce police resources and make policing more efficient and effective. However, this practice is fraught with ethical peril. Human rights and civil liberties groups warn that because these algorithms are trained on historical police data - which often reflects past and present human biases - they risk perpetuating and amplifying discriminatory policing practices, disproportionately targeting marginalized and minority communities. This raises fundamental questions about due process, the presumption of innocence, and the potential for creating a "dystopian future of ubiquitous state surveillance".[12]

The divergence in these two regulatory spheres creates a significant risk. A technology deemed ethically unacceptable for domestic law enforcement, such as a fully autonomous facial recognition and tracking system, might be developed and perfected in a less-regulated military context, only to later "trickle down" into policing. This feedback loop, where norms established in one domain bleed into the other, threatens to erode civil liberties and normalize levels of surveillance and automation that would otherwise be rejected by democratic societies.

Funding the Future: The Technology-Budget Nexus

The imperative to modernize is colliding with significant financial realities in both law enforcement and the military. Local and state police agencies often face severe budget constraints that hinder the adoption of crucial new technologies. One proposed solution is the strategic reallocation of salary savings from the large number of chronic, unfilled officer positions to fund technology programs that can act as "force multipliers."[13] For example, the annual cost of one vacant officer position could fund an extensive network of Automated License Plate Readers (ALPRs) or a Drone-as-First-Responder program, enhancing the capabilities of the existing force. While this offers a potential short-term solution, agencies remain heavily reliant on a complex and competitive landscape of federal, state, and private grants to fund major technological upgrades.

Military organizations face a similar, though larger-scale, challenge. Even with rising topline budgets, defense leaders are forced to make difficult trade-offs between three competing priorities: force size (the number of personnel, ships, and aircraft), modernization (research, development, and procurement of next-generation systems), and readiness (training, maintenance, and sustainment of the current force).[14] The immense cost of new platforms, such as advanced fighter jets and naval vessels, can consume the majority of available funding, forcing a slowdown in the overall pace of modernization across the force. This can lead to difficult choices, such as maintaining the readiness of an aging and increasingly obsolete force at the expense of investing in the technologies needed to compete with advanced adversaries.[14]

IV. The Threat Multiplier: Climate Change and Environmental Stress

Climate change is no longer a peripheral environmental issue but a central driver of global insecurity. Its impacts are systemic, affecting everything from geopolitical stability to the operational readiness of military and public safety forces.

An Accelerant of Instability

The U.S. Department of Defense, along with numerous other national intelligence and security agencies, has formally identified climate change as a "threat multiplier".[15] This concept posits that climate change does not typically cause conflict on its own but acts as a powerful accelerant of instability, amplifying and worsening existing stressors such as poverty, environmental degradation, political fragility, and social tensions.

The direct physical impacts of a warming planet are projected to have vast geopolitical consequences. Increasing food and water scarcity, particularly in already vulnerable regions, can fuel competition and conflict over essential resources. The proliferation of disease vectors and the permanent loss of habitable land due to sea-level rise are expected to trigger mass migration flows, creating new refugee crises that can strain the capacity and stability of both origin and destination countries.

This process represents a direct assault on the fundamental contract between a state and its citizens: the ability to provide basic security and deliver essential services. The DNI's Global Trends report notes that states are already struggling to meet the rising expectations of their populations.[1] When a government repeatedly fails to protect its people from predictable and escalating climate-related disasters - when infrastructure collapses in floods, emergency services are overwhelmed by wildfires, or food and water supplies become insecure - its legitimacy erodes. This erosion of state capacity creates a power vacuum. In this vacuum, non-state actors, from criminal organizations and terrorist groups to private corporations, can step in to provide the services and security that the state cannot, winning the loyalty of the population and challenging the state's sovereignty from within. In this context, climate adaptation is not merely an environmental policy but a core mission for state survival and a critical component of public safety and national security.

Impacts on Operational Readiness and Infrastructure

Beyond its role as a geopolitical destabilizer, climate change poses a direct physical threat to the infrastructure and operational readiness of security forces. Military installations are particularly vulnerable. Coastal naval bases, such as the U.S. Navy's largest port in Norfolk, Virginia, are directly threatened by rising sea levels and more frequent storm surges, calling into question their long-term viability.[15] Inland bases are not immune, facing increased risks from wildfires, droughts, and extreme temperatures that can damage critical assets, disrupt vital training schedules, and endanger personnel.

This vulnerability extends to the civilian infrastructure upon which both military and public safety responders depend. Roads, bridges, power grids, and communication networks are all susceptible to damage from more intense and frequent extreme weather events, which can cripple the ability of forces to deploy and respond effectively during a crisis. Furthermore, the escalating frequency of large-scale natural disasters is placing an unsustainable strain on resources. Military and emergency response agencies are being called upon more often to conduct large-scale humanitarian assistance and disaster relief (HADR) missions, both domestically and internationally. This increased operational tempo stretches personnel and equipment thin, potentially degrading their readiness for other core national security missions.

The global response to climate change - the transition away from a fossil-fuel-based economy - is itself becoming a new arena for geopolitical competition. This "green transition" is fundamentally reordering global power

dynamics. For a century, geopolitics has been shaped by the control of oil and gas resources. The new cornerstones of power will be the critical minerals (lithium, cobalt, rare earths) and manufacturing capacity required for batteries, solar panels, and wind turbines. This shift is creating new economic dependencies and reconfigured value chains, as a nation's reliance on foreign oil may simply be replaced by a reliance on foreign-made batteries or processed minerals. This will inevitably drive new alliances, new resource-based conflicts, and new priorities for defense and intelligence agencies tasked with securing these new, critical supply chains.

V. The Foundation at Risk: Internal and Institutional Challenges

While external threats are multiplying, public safety and defense institutions are simultaneously being weakened from within by a series of profound institutional challenges. A crisis in human capital, an erosion of public trust, and persistent budgetary dilemmas are undermining the very foundation of national and community security.

The Human Capital Crisis: Recruitment and Retention

Both military and law enforcement organizations, particularly in Western nations, are facing a severe and sustained crisis in their ability to recruit and retain personnel. This is not a cyclical downturn but a structural problem with deep roots and significant strategic implications. The U.S. military, for example, has experienced several consecutive years of recruiting shortfalls, creating a significant national security challenge.[16] The causes are multifaceted and complex. There is a declining propensity for military service among young people, driven by factors such as declining trust in institutions, debates over post-9/11 wars, and shifting views on collective responsibility. This is compounded by a shrinking pool of eligible candidates; only about one in four Americans between the ages of 17 and 24 meet the required physical, educational, and moral standards for service.[16] Intense competition from a strong private labor market further complicates recruiting efforts. In response, the services are implementing a range of initiatives, including larger enlistment bonuses, preparatory courses to help ineligible candidates meet standards, and new marketing campaigns, such as the revival of the Army's "Be All You Can Be" slogan.

Law enforcement agencies are facing a parallel crisis. A 2024 survey by the International Association of Chiefs of Police (IACP) found that over 70% of U.S. agencies report that recruitment has become more difficult compared to five years ago, with departments on average operating at 91% of their authorized strength.[17] The profession has seen a surge in resignations and retirements, with many officers leaving within their first five years of service. The top reasons cited for these departures include higher pay at other agencies, a lack of career growth opportunities, general dissatisfaction with policing as a career, and concerns about work-life balance and burnout.[17] The staffing shortage has forced some agencies to lower hiring standards and has led to the reduction or elimination of specialized units and community engagement programs, prioritizing essential patrol functions.

The true danger of this retention problem is the "experience drain" it creates.[17] The departure of officers in their first five years, combined with a wave of retirements among the most senior personnel, is hollowing out the critical middle tier of experienced officers and non-commissioned officers. These are the individuals who possess the judgment and institutional knowledge to mentor new recruits, serve as field training officers, and make sound tactical decisions under pressure. Their loss is a strategic vulnerability that degrades operational effectiveness and increases institutional risk far more than raw headcount numbers would suggest. It is not just a shortage of bodies, but a critical shortage of experience and sound judgment.

The Legitimacy Deficit: Public Trust and Procedural Justice

The human capital crisis is inextricably linked to a deeper crisis of legitimacy. Public trust and confidence are the bedrock of effective policing and a vital component of national cohesion, yet this foundation is showing signs of severe erosion in many parts of the world. Global polls show that while confidence in local police has seen

modest increases recently, it remains fragile and varies widely by region and demographic group.[18] In many nations, a significant trust deficit persists, particularly among younger generations and racial and ethnic minority communities, who often perceive law enforcement as lacking lawfulness and legitimacy based on their personal and vicarious experiences.

This loss of trust has severe consequences, undermining the ability of police to function effectively. Without legitimacy, public cooperation diminishes, making it harder to solve crimes and maintain social order. An extensive body of criminological research has established a powerful link between "procedural justice" and "police legitimacy".[19] Procedural justice refers to the public's perception that police exercise their authority fairly. It is commonly defined by four key tenets: giving people a voice (listening to their side of the story), demonstrating neutrality (making decisions based on facts, not bias), treating people with respect, and showing trustworthiness (acting in the community's best interest).[19] When the public perceives that police are acting in a procedurally just manner, they are more likely to view the police as legitimate and are therefore more willing to cooperate and obey the law. As a result, policies and training aimed at enhancing procedural justice have become a central pillar of modern police reform efforts. This includes training on implicit bias and de-escalation, as well as concrete community engagement strategies such as "Coffee with a Cop" programs, increased foot patrols, and greater transparency through the public release of data and policies.

The recruitment and legitimacy crises are not separate problems; they are locked in a dangerous, mutually reinforcing feedback loop. Low public trust and a negative perception of the profession make it incredibly difficult to recruit qualified and diverse candidates from the very communities that need to be served. As agencies become critically understaffed, the remaining officers become overworked, stressed, and have less time for the proactive community engagement that is essential for building trust. This can lead to more negative, enforcement-focused interactions with the public, which in turn further erodes legitimacy and makes future recruitment even harder. Breaking this downward spiral requires more than just better pay or advertising; it demands fundamental, sustained reforms that restore the institution's legitimacy in the eyes of the public from which it must recruit.

The Modernization Dilemma

The challenge of modernizing forces in the face of new threats is compounded by intense budgetary pressures. Defense leaders must constantly navigate a difficult set of trade-offs between three competing priorities: Force Size, Modernization, and Readiness.[14]

Force Size refers to the total number of personnel and major weapon systems (e.g., brigades, ships, aircraft squadrons). This is often the easiest element to cut to save money, but doing so risks creating a military that is too small to sustain operations in a major, protracted conflict.

Modernization involves the research, development, and acquisition of next-generation technologies and platforms to maintain a qualitative edge over adversaries. Prioritizing modernization at the expense of the other two areas can lead to a "hollow force" equipped with advanced but poorly maintained systems and operated by undertrained personnel.

Readiness encompasses the training, maintenance, logistics, and sustainment required to ensure the current force is prepared to fight effectively on short notice. Over-investing in readiness for today's force can mean forgoing the modernization necessary to be competitive tomorrow, resulting in a highly proficient but technologically obsolete military.

This high-stakes balancing act is a persistent dilemma for defense planners. The extraordinarily high cost of modern weapon systems means that procuring new ships or aircraft can consume the majority of the available budget, leaving little for the readiness of the rest of the fleet or for increasing the overall size of the force.[14]

VI. The Interoperability Imperative: Overcoming Barriers to Collective Security

In an era of transnational threats and coalition warfare, the ability of different security organizations to operate together effectively is not a luxury but a strategic necessity. This challenge of interoperability exists at both the international level, among allied militaries, and at the domestic level, among different public safety agencies responding to a common crisis.

Allied Defense and Deterrence

For a multinational alliance like the North Atlantic Treaty Organization (NATO), interoperability is the very foundation of credible collective defense and deterrence. NATO defines interoperability as "the ability to act together coherently, effectively, and efficiently to achieve Allied objectives".[20] This capability is built upon three distinct but interconnected dimensions:

- **Technical Interoperability:** The ability of systems, networks, and equipment to exchange data and services. Can a Norwegian radar system seamlessly pass targeting data to a German air defense unit?
- **Procedural Interoperability:** The alignment of common doctrines, tactics, techniques, and procedures. Do different national forces follow the same rules of engagement and operational planning processes?
- **Human Interoperability:** The ability of personnel to communicate effectively, understand each other's command cultures, and build mutual trust through combined training and operations.[20]

Despite decades of effort, significant challenges to interoperability persist across all three dimensions. Vast technological disparities exist between allies; within NATO, there are at least 13 different battle-tracking systems, many of which are not compatible with one another.[21] Doctrinal differences, for example in how different armies employ artillery, can create dangerous friction on the battlefield. Gaps in logistical capabilities and human factors, from simple language barriers to more complex cultural differences in command philosophy, also remain major hurdles. To address these issues, NATO relies on a continuous cycle of large-scale joint exercises, such as the Coalition Warrior Interoperability Exercise (CWIX), which provides a controlled environment for nations to test their systems and procedures, identify shortfalls, and implement fixes before they are needed in a real-world crisis.

Domestic Emergency Response

A parallel challenge exists within nations, where a persistent failure in major emergencies - from terrorist attacks like 9/11 to large-scale natural disasters - is the inability of different public safety agencies (police, fire, emergency medical services) to communicate and coordinate effectively. While outdated or incompatible radio technology is often blamed, the root causes are frequently organizational and political rather than technical. These include institutional "turf issues" over the management and control of communications systems, a lack of shared priorities for interoperability among senior government leaders, and a history of "stove-piped" system development where each agency builds its own network without regard for inter-agency needs. The scale of the problem is immense; in the United States alone, there are over 6,000 separate 911 call centers, many using different computer-aided dispatch (CAD) systems that cannot easily share critical information during a multi-jurisdictional incident, leading to delays and inefficiency when lives are on the line.[22]

At the heart of this interoperability challenge, both internationally and domestically, lies a fundamental paradox of sovereignty. The modern threats that security organizations face - hybrid warfare, cyberattacks, terrorism, pandemics, and climate-fueled disasters - are inherently transnational and do not respect jurisdictional or national borders. To counter these borderless threats effectively, organizations and nations must cede a degree of operational sovereignty by adopting common standards, sharing sensitive data, integrating command structures, and procuring compatible equipment. However, the political and institutional impulse is often to protect local control, support domestic industries, and retain sovereign command over all assets. This tension between the need for deep integration and the desire for sovereign control is the central, enduring challenge of collective security. Overcoming it depends less on finding a perfect technical solution and more on generating the political will to prioritize shared security over institutional autonomy.

VII. Strategic Imperatives and Recommendations for a Resilient Future

The convergence of geopolitical, technological, environmental, and institutional challenges has created a security environment of unprecedented complexity and volatility. Navigating this era requires moving beyond incremental adjustments to existing models and embracing a new strategic framework for security and resilience. The following imperatives offer a path forward for leaders in the Public Safety and Defense sectors.

Embrace a "Whole-of-Society" Resilience Model: Security can no longer be the exclusive domain of siloed government agencies. The nature of modern threats, particularly hybrid warfare, cyberattacks, pandemics, and the systemic shocks of climate change, demands a comprehensive, "whole-of-society" approach. This involves actively mobilizing and integrating the capabilities of the private sector, civil society organizations, academia, and the public. Governments must act as facilitators, fostering public-private partnerships to protect critical infrastructure, promoting media literacy to counter disinformation, and building community-level preparedness to ensure that society can withstand and recover from major disruptions.

Rebuild the Foundation: Prioritize Human Capital and Legitimacy: The concurrent crises in recruitment, retention, and public trust are not peripheral issues; they are strategic vulnerabilities that undermine the very foundation of security institutions. A paradigm shift is required. This means moving beyond short-term incentives to make aggressive, sustained investments in the quality of life, mental health support, and modern career paths for uniformed personnel. Crucially, this must be coupled with a radical and unwavering commitment to transparency, accountability, and procedural justice. Rebuilding legitimacy is not a public relations exercise; it is a strategic imperative for solving the human capital crisis at its root and ensuring the long-term viability of the all-volunteer force and professional policing.

Foster Strategic Interoperability by Design: The persistent failures in inter-agency and international cooperation demonstrate that retrofitting interoperability onto disparate systems and organizations is a costly and often ineffective approach. The strategic imperative is to embed interoperability "by design" from the very beginning of any new capability development. For alliances like NATO, this means prioritizing common standards, data-sharing protocols, and collaborative procurement to avoid creating new technological divides. For domestic public safety, it requires strong leadership from national and regional governments to drive the adoption of open-architecture standards for communications and data systems, breaking down the institutional stovepipes that hinder effective joint response.

Navigate the Technological Revolution Ethically: The rapid advance of AI and other disruptive technologies is outpacing the development of legal and ethical frameworks to govern their use. There is an urgent need to establish robust, independent national and international bodies to create clear ethical guardrails and legal accountability mechanisms before these technologies are widely deployed in the security domain. This involves a multi-stakeholder dialogue including technologists, ethicists, human rights experts, and security

practitioners. The goal must be to ensure that the pursuit of technological advantage and operational efficiency does not come at the cost of fundamental human rights, democratic values, and meaningful human control over the use of force.

Adopt Adaptive Budgeting for a Hybrid Age: The "strategic squeeze" between the demands of conventional, industrial-scale conflict and ambiguous, information-age warfare requires more agile and adaptive budgeting models. Rigid, long-term budget plans are ill-suited to a volatile environment. Defense and security organizations should explore creating flexible funding pools that can be rapidly allocated to counter emerging threats, prioritizing investments in dual-use technologies that serve both conventional and irregular warfare needs, and protecting funding for the long-term research and development that will define the next generation of conflict.

Citerede værker

1. National Intelligence Council. (2021). *Global Trends 2040: A More Contested World*. Tilgået oktober 8, 2025,(https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf)
2. PwC. (n.d.). *Five megatrends and their implications for global defense & security*. Tilgået oktober 8, 2025, https://www.pwc.com/gx/en/industries/government-public-services/megatrends-defence-security.html
3. FinancialContent. (2025). *Global defense industry soars amid geopolitical turmoil, but supply chains loom large*. Tilgået oktober 8, 2025, http://markets.financialcontent.com/stocks/news/read/44478174
4. International Journal of Humanities and Social Sciences. (n.d.). *The Economic Impact of Geopolitical Crises on Defense Supply Chains*. Tilgået oktober 8, 2025,(https://www.ijhess.com/paper/vol-13-issue-2/4.IJHESS_130204.pdf)
5. NATO Foundation. (2020). *Hybrid Warfare and NATO*. Tilgået oktober 8, 2025,(https://natofoundation.org/wp-content/uploads/2020/07/GC-2020-Dossier-Hybrid-Warfare.pdf)
6. Center for Strategic and International Studies. (2025). *Will, Cohesion, Resilience, and the Wars of the Future*. Tilgået oktober 8, 2025, https://csis.org/analysis/will-cohesion-resilience-and-wars-future
7. Danish Security and Intelligence Service. (n.d.). *How to counter the hybrid threat*. Tilgået oktober 8, 2025, https://pet.dk/publikationer/how-to-counter-the-hybrid-threat
8. Institute for Economics & Peace. (2024). *Global Terrorism Index 2024*. Tilgået oktober 8, 2025,(https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-2.pdf)
9. U.S. Department of Justice. (2024). *FACT SHEET: Disruptive Technology Strike Force Efforts In First Year*. Tilgået oktober 8, 2025, https://www.justice.gov/opa/pr/fact-sheet-disruptive-technology-strike-force-efforts-first-year-prevent-sensitive
10. Center for Strategic and International Studies. (2025). *War and the Modern Battlefield*. Tilgået oktober 8, 2025, https://features.csis.org/war-and-the-modern-battlefield/
11. International Committee of the Red Cross. (n.d.). *Autonomous weapon systems under international humanitarian law*. Tilgået oktober 8, 2025, https://www.icrc.org/en/document/autonomous-weapon-systems-under-international-humanitarian-law-legal-perspective
12. Centre for International Governance Innovation. (n.d.). *The Promises and Perils of Predictive Policing*. Tilgået oktober 8, 2025, https://www.cigionline.org/articles/promises-and-perils-predictive-policing/
13. Police Chief Magazine. (n.d.). *Enhancing Public Safety with Technology*. Tilgået oktober 8, 2025, https://www.policechiefmagazine.org/enhancing-public-safety-with-technology/
14. National Defense Magazine. (2025). *COMMENTARY: The Most Important Trade-Offs: Force Size vs. Modernization vs. Readiness*. Tilgået oktober 8, 2025, https://www.nationaldefensemagazine.org/articles/2025/1/28/commentary-the-most-important-trade-offs-force-size-vs-modernization-vs-readiness
15. The White House. (2015). *The National Security Implications of a Changing Climate*. Tilgået oktober 8, 2025, https://obamawhitehouse.archives.gov/the-press-office/2015/05/20/fact-sheet-national-security-implications-changing-climate
16. U.S. Government Accountability Office. (2023). *DOD Actions Needed to Address Recruitment and Retention Challenges*. Tilgået oktober 8, 2025, https://www.gao.gov/products/gao-23-106551
17. Lexipol. (2025). *The State of Police Recruitment and Retention: A Continuing Concern*. Tilgået oktober 8, 2025, https://www.lexipol.com/resources/webinars/state-of-police-recruitment-retention-2025/
18. Gallup. (2023). *Confidence in Police Rises, but World Doesn't Feel Safer*. Tilgået oktober 8, 2025, https://news.gallup.com/poll/513139/confidence-police-rises-world-doesn-feel-safer.aspx
19. Oxford Research Encyclopedia of Criminology and Criminal Justice. (2025). *Procedurally Just Policing and Police Legitimacy*. Tilgået oktober 8, 2025, https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-2

20. NATO Allied Command Transformation. (n.d.). *Interoperability: A Cornerstone Concept*. Tilgået oktober 8, 2025, https://www.act.nato.int/interoperability

21. U.S. Army War College Press. (2025). *Measuring Interoperability within NATO*. Tilgået oktober 8, 2025, https://publications.armywarcollege.edu/pubs/3785.pdf

22. U.S. Department of Homeland Security. (2024). *Interoperability is Key to Effective Emergency Communications*. Tilgået oktober 8, 2025, https://www.dhs.gov/science-and-technology/news/2024/04/18/feature-article-interoperability-key-effective-emergency