MITSEMINAR XXI
EDUCATING U.S. NATIONAL SECURITY LEADERS

EMERGING TECHNOLOGIES
January 5, 2026
READING NOTES

ARTIFICIAL INTELLIGENCE

In a 2023 report for Harvard University's Belfer Center, **Issam Eddine Abail et al.** provide an overview of artificial intelligence (AI) and machine learning (ML). They define the former as "the theory and application of machines—especially computer programs—to perform tasks that typically require human intelligence." They define ML as a subfield of AI that relies on "automatic discovery of historical patterns in data using statistical algorithms."

The authors argue that recent AI development has been spurred by 1) better computer hardware; 2) internet-enabled data availability and cloud computing; 3) sensor improvements; 4) the internet of things; and 5) improved algorithms. The end result is that AI models can be trained much faster on much larger amounts of data from a much larger number of inputs. These five accelerators, in particular, advantage ML approaches to AI development.

The authors write that, despite the prodigious advancements made in AI technology over the last decade, current AI applications are *narrow*, meaning that AI is applied to individual tasks, like text generation. Artificial general intelligence, in contrast, means AI that can move between domains like humans do. The report cautions that "real AGI is still not foreseeable in the near future."

Greg Allen and Taniel Chan, writing in 2017, highlight a number of military implications of AI development, focusing on autonomous systems and cyberwarfare. First, they argue that AI development will dramatically improve the capabilities of autonomous robotics, including drones and missiles. They write, "The size, weight, and power constraints that currently limit advanced autonomy will eventually be overcome, just as smartphones today deliver what used to be supercomputer performance." The combination of increasing capability and falling cost means that autonomous military systems will transform conflict.

Second, they posit that AI improvements will lead to greatly improved cyberwarfare capabilities. AI's promise in this arena is a reduction in the number of humans needed for cyberwar while increasing the speed of military response. Third, Allen and Chan assert that both offensive and defensive capabilities will be strengthened, and that even non-state actors will be able to take advantage of these improvements.

The authors close with ten potential transformative scenarios, which envision worlds in which military power is revolutionized by AI advances. These ten scenarios are: 1) lethal autonomous weapons form the bulk of military forces; 2) disruptive swarming technologies render some military platforms obsolete; 3) robotic assassination is common and difficult to attribute; 4) mobile-robotic-improvised explosive devices grant low-cost, precision guided munition-like capabilities to terrorists; 5) military power grows disconnected from population size and economic strength; 6) cyberweapons are frequently used to kill; 7) most actors in cyberspace will have no choice but to enable relatively high levels of autonomy, or else risk being outcompeted by "machine-speed" adversaries; 8) unexpected interactions of autonomous systems cause occasional "flash crashes"; 9) involving machine learning in military systems will create new types of vulnerabilities and new types of cyberattacks that target the training data of machine learning systems; and 10) theft and replication of military and intelligence AI systems will result in AI cyberweapons falling in the wrong hands.

Adib Bin Rashid et al., in a 2023 review article, outline how AI developments will influence military operations. They detail seven AI "patterns"—i.e., capability areas in which AI operates: 1) hyper-personalization; 2) pattern recognition; 3) conversation and human interaction; 4) predictive analytics and decisions; 5) goal-driven systems; 6) autonomous systems; and 7) anomaly detection. Applied to military endeavors, these seven patterns enable a wide spectrum of improved capabilities, ranging from improved weapon targeting to better surveillance to more streamlined logistics. The authors argue, "practically every military application involves artificial intelligence." The authors close with a note of caution. They argue that AI may compromise strategic stability by intertwining nuclear and non-nuclear systems and by greatly accelerating the tempo of military decision-making. Moreover, due to the black box nature of AI algorithms, understanding the signaling behind adversary military posture becomes much more difficult.

In a 2022 RAND report, **Todd C. Helmus** argues that "disinformation is getting an upgrade." Helmus warns that the proliferation of deepfake algorithms, which can modify or generate realistic images of real-life individuals, will only worsen America's existing disinformation-related problems. When any individual with a computer can create a synthetic video of political figures or military officials, truth in online forums becomes blurred. The author argues that we have yet to see truly disruptive deepfakes but that technological advances make their arrival inevitable. Moreover, given the improved speed of AI and reduced need for humans, even more disinformation will circulate online.

Erik Lin-Greenberg examines the challenges to alliances and multinational operations posed by AI in his 2020 article for the *Texas National Security Review*. He argues that AI both increases the complexity of multinational operations and provides adversaries with a tool to sow mistrust among partners in a high-speed decision environment. The first challenge for alliances is operational coordination. Allied states will have to account for different ethical standards on military applications of AI, different rates of adoption of AI, and technical and data-sharing concerns. Second, AI can be used by adversaries to launch deception campaigns to divide alliance partners. AI-manipulated audio and videos, known as deepfakes, could disrupt effective alliance command and control, especially in a multinational environment where commanders have limited previous experience cooperating with their foreign partners and language barriers may exist. To reduce these risks, alliance partners need to establish standards for AI data management, data-sharing, AI applications in the military, pre-delegate to commanders to increase the speed of response in an AI-enabled wartime environment and invest in technology to detect deepfakes.

In a 2020 RAND report, **Forrest E. Morgan et al.** examine the military implications of AI, drawing upon data gleaned from several dozen interviews with AI experts and a survey of 2,500 Americans. The report focuses on changes to warfighting, ethical concerns, and action by U.S. rivals. They reach seven findings. First, there exists no consensus on a timeline for the militarization of AI, nor a consensus on how AI will affect military operations. Second, unlike in past technological advancements, the U.S. does not have either a monopoly or a first-mover advantage in AI. Both China and Russia are moving quickly in this arena. Third, military AI offers three types of risk: ethical, operational, and strategic. For each type of risk, military AI holds the risk of accident and poses challenges to making sure that systems follow the commander's intent. Fourth, international competition incentivizes countries, including the United States, to push fast on AI development without sufficient attention to safety and reliability concerns. Fifth, the U.S. public supports DoD research into AI but is concerned about specific use cases, like lethal autonomous decision making. Sixth, significant international AI arms control is unlikely. Seventh, even American rivals recognize that military AI carries risks and must be supervised by humans.

Morgan et al. further argue that the United States is likely to be more constrained by ethical concerns on military AI than are Russia and China. However, they still recommend that the U.S. should continue to abide by the laws of armed conflict and the guidelines of just-war doctrine. They also recommend that the United States should attempt confidence-building and risk-reduction measures with China and Russia.

Rebecca Crootof argues that concerns about autonomous weapons have highlighted a central problem in international humanitarian law (IHL): the allowance for incidental civilian harm. IHL explicitly permits acts that cause civilian harm incidentally. Foreseeable and extensive civilian harm is allowed under IHL so long as it is caused by attacking a legitimate military target. New technologies have both expanded the number of legitimate military targets that may cause incidental civilian harm (electrical and telecommunications infrastructure) and expanded the possibilities for incidental harm. Precision strikes, for example, while reducing civilian casualties in a strike, increase the number of strikes with incidental harm, justified by their more limited collateral damage. New technologies also introduce a variety of new sources for error, both human and technical, that can result in unintended casualties. This problem of accountability for AI highlights the need to rectify the allowance for incidental civilian harm under IHL. To address this problem and the challenge posed by AI for accountability under IHL, Crootof recommends adopting a "war torts" model in which states are held responsible by international courts for incidental civilian harm caused during war.

In *Foreign Affairs,* **Ben Buchanan and Tantum Collins** explain the importance of the United States winning the AI race and the challenge of doing so. They argue that, thus far, AI investment has been driven by the private sector. However, going forward, the government will need to support private sector investment with public sector investments in energy infrastructure, talent development, and security against foreign espionage efforts. By 2028, AI data centers could use up to 12% of America's electricity production. Without government-led investments in electricity infrastructure, AI progress will be slowed. Although the Biden administration supported grid-expansion efforts through the Build Back Better Act, Trump's Big Beautiful Bill gutted many of these programs. Without more energy capacity, AI companies may host their data centers elsewhere, making the United States dependent on foreign energy infrastructure for the military and economic dividends of AI technology. Second, foreign-born scientists are key to the United States' strength in AI development. More than 70% of US-based AI researchers were born abroad. Although the United States has an edge over China in access to advanced AI chips, it lags in energy infrastructure and civil-military fusion of the AI sector. In exchange for government assistance in preventing espionage, developing energy infrastructure, and talent development, AI companies should help the national security apparatus incorporate AI technologies.

SYNTHETIC BIOLOGY

In **Gopal et al.**, the authors examine preparedness for two types of pandemics: a *wildfire* pandemic and a *stealth* pandemic. A *wildfire* pandemic resembles the COVID-19 outbreak with a lethal, highly transmissible virus quickly spreading throughout the population. Sufficient stockpiles of pandemic-proof personal protective equipment (P4E) can insulate a population from the worst effects of this pandemic. However, humanity is less prepared for *stealth* pandemics. A *stealth* pandemic resembles HIV, where a deadly virus with a long incubation period rapidly spreads through the population before being discovered. Here, early warning using metagenomic sequencing, the credibility of expert leaders, well-funded medical research, P4E, and pandemic-proofed buildings with germicidal lights and ventilation are key. With pandemics occurring roughly every 33 years historically, the authors argue that preparing for the next one is not just a precaution, but rather is a necessity that will save lives.

In a harrowing report, **Kevin M. Esvelt** argues that the knowledge and skills necessary to create new pandemic-capable pathogens are diffusing rapidly. He estimates that within a decade, "tens of thousands" of individuals will have the capability to generate multiple pandemics. The simultaneous unleashing of multiple pandemic-capable pathogens would threaten worldwide catastrophe and the survival of civilization.

To forestall the worst-case outcomes, Esvelt outlines a three-prong strategy: delay, detect, and defend. *Delay* would be accomplished through universal DNA synthesis screening and a test-ban treaty on pandemic-capable pathogens. *Detect* is accomplished by sequencing potential threats to identify any future pandemics before they spread. *Defend* would require developing extreme pandemic preparedness measures, including stockpiling high-quality personal protective gear for essential workers, improving supply chain resiliency, and the installation of germicidal lights.

As the assigned overview reading indicates, t**he CDC and USDA** jointly operate the Federal Select Agent Program (FSAP), with the CDC overseeing threats that cause disease in humans while the USDA regulates those that cause disease in animals and plants. The FSAP regulates "the possession, use, and transfer of biological select agents and toxins that have the potential to pose a severe threat to public, animal or plant health, or to animal or plant products," as well as authorizes certain laboratories to work on these agents.

Jaime M. Yassif et al. highlight efforts to prevent the misuse of DNA synthesis technology. They argue that "safeguards for DNA synthesis technology—to ensure that providers do not inadvertently sell the building blocks of dangerous pathogens to malicious actors—have not kept pace with growing global demand for this service and declining costs." The authors note that no national government requires screening DNA synthesis orders; as a result, private actors—like the Nuclear Threat Initiative—are attempting to rally synthesis providers to create guidance for customer screening.

In a 2019 article, **Gregory Lewis et. al.** argue that biological information, rather than biological material, should be the principal security concern. They suggest that existing biosecurity approaches are poorly suited to manage hazardous biological information and recommend new policies. Departing from traditional academic values of free dissemination of research, the authors contend that new scientific research should only be disclosed should its expected gain exceeds the likely hazard.

Writing recently in *Nature*, **Jaspreet Pannu et al**. caution that AI tools could dramatically increase the risk of future pandemics. They write that large language models (LLMs) like GPT-4o, combined with ready access to DNA synthesis facilities, allow non-experts to create dangerous biological agents, like more lethal pathogens. They argue that the leading AI companies are, by-and-large, self-regulated, an approach insufficient to the gravity of the task.

Pannu et al. argue for a regulatory approach that seeks to minimize "those harms that could result in the greatest loss of life and disruption to society," referring mainly to transmissible pathogens. Under such a regulatory framework, AI developers would need to specify which AI capabilities are most likely to lead to pandemic-scale harm and how those capabilities can be safeguarded against.

In a just-released piece in *Science*, **Katarzyna P. Adamala** et al. warn about the risks of creating "mirror life." The authors begin by explaining that all known life is homochiral, which means that the building blocks that compose organic material are not symmetrical. In other words, biological agents like amino acids and DNA cannot be superimposed upon their mirror images. This basic fact of life creates an interesting, but until now fully theoretical, possibility: could humans engineer mirror life, life composed of biological agents with reversed chirality?

While mirror life might seem like a harmless thought experiment, Adamala et al. warn that mirror bacteria could potentially cause extremely lethal infections in humans and other animals. They write:

> Although we were initially skeptical that mirror bacteria could pose major risks, we have become deeply concerned. We were uncertain about the feasibility of synthesizing mirror bacteria but have concluded that technological progress will likely make this possible. We were uncertain about the consequences of mirror bacterial infection in humans and animals, but a close examination of existing studies led us to conclude that infections could be severe. Unlike previous discussions of mirror life, we also realized that generalist heterotroph mirror bacteria might find a range of nutrients in animal hosts and the environment and thus would not be intrinsically biocontained.

RECOMMENDED

Artificial Intelligence

In this memorandum, President **Joe Biden** gives guidance to the Executive Branch on "appropriately harnessing artificial intelligence (AI) models and AI-enabled technologies in the United States Government, especially in the context of national security systems (NSS), while protecting human rights, civil rights, civil liberties, privacy, and safety in AI-enabled national security activities."

Synthetic Biology

In **Endy et al.** (2025), the authors put forth a strategy to counter biosecurity threats in the 21st century. The authors argue that the proliferation of advances in biotechnology, while enabling scientific achievements, has also increased the potential for bio-attacks. Building a virus from scratch has been feasible since the beginning of the millennium, as is often pointed out in debates about the origins of COVID-19. Most countries have officially ended their bioweapons programs. However, North Korea and Russia maintain active bioweapons programs, and China and Iran are suspected of being noncompliant. The vulnerability to biological threats has been exacerbated by recent trends in public health in the United States, most notably the anti-vax movement.

Critical to countering bio-threats is a system of active surveillance through genomic sequencing, a robust capability for vaccine development, widespread availability of diagnostic tests, and advances in treatments are all ways biotechnology advances can be used to counter biological threats. The authors make several recommendations, including creating an intelligence agency focused on biological threats, creating a domestic agency charged with auditing biological research for safety to restore public trust, disallowing most research on pandemic-potential pathogens (e.g., coronaviruses) to reduce the risk of lab-based outbreaks, and convening allies and adversaries to reaffirm the importance of upholding the Biological Weapons Convention.

A 2022 report by the **Congressional Research Service (CRS)** reviews the challenges posed by synthetic biology, which it defines as "the application of engineering principles and the use of systematic design tools to enable the reprogramming of cellular systems at the genetic level for a specific functional output." The CRS cautions that the full extent of synthetic biological capabilities has not yet been realized, but it identifies five different areas of synthetic biological applications: biomanufacturing, agriculture, environmental conservation, cell-free systems, and climate change mitigation.

Advances in synthetic biology, according to CRS, have led to several biosecurity challenges. The increased ability of scientists to modify the genomes of viruses and bacteria increases the risk of designed pathogens. Even with benign applications of synthetic biology, like gene drives designed to reduce the population of mosquitoes, risk of unintended consequences that proliferate through the environment. The CRS notes, "if a staple crop or ecosystem were impacted by a synthetic biology application, deliberately or by accident, it could affect U.S. food and water supply chains and global food security systems."

In the 2023 *Biodefense Posture Review*, **the United States Department of Defense** identifies several areas of biothreat: 1) naturally occurring biological threats, like a normal infectious disease pandemic; 2) accidental biological threats, which can involve pathogens released by laboratory accidents; and 3) deliberate biological threats, which result from bioweapon programs. The report states, "The United States assesses that North Korea and Russia maintain offensive biological weapons programs in violation of Biological Weapons Convention (BWC) obligations and identifies concerns with Iran's activities and its compliance with the BWC."

The DoD states that the U.S. military has extensive experience operating during times of pandemic and in places with dangerous endemic diseases. From those experiences, the U.S. military has learned to prioritize force health protection measures. However, the report cautions that such measures are unlikely to be effective against future pathogens resistant to medicines, whether those pathogens arise naturally or through bioengineering.