# EMERGING TECHNOLOGIES IN DEFENCE: AI, AUTONOMY, AND CYBERSECURITY

Interview with

## BRIG (RET.) NICK COWEY MBE

*Former Head of Military Capability Delivery*
*British Army HQ*

iDeaS BY COGES EVENTS

Powered by ABLO CONSULTING

**Drawing from your extensive experience, how has the military's integration of technology, especially AI and robotics, evolved over the years, and how do you see it complementing the human elements in operations?**

Militaries have been integrating new technology for as long as humans have fought, which is all our history really. My own former unit, the Royal Tank Regiment, owes its formation to one of the most famous new technological battlefield innovations – the tank. Meanwhile my career in the British Army has correlated closely with the period of digitisation and digitalisation of military capability, I joined a largely analogue and unconnected force and left one which has become networked and digitised, although not perhaps as much as the civilian world it exists in. Within a connected force, the possibilities of automation, robotics and more recently machine learning and AI have all grown.

Early use of robotics and automation seemed to focus on tasks deemed too dangerous or dull for humans, such as bomb disposal, surveillance, and logistics. More recently un-crewed systems have proliferated in every domain and modern militaries use robotic systems for air (UAVs), ground (UGVs) and underwater (UUVs). They have expanded from their initial roles in intelligence gathering and reconnaissance, to increasingly become lethal systems. Drones, have evolved quickly, partly driven by the civilian consumer market to possess greater autonomy, enabling them to perform complex tasks without constant human intervention – where drones were once flown, they now fly themselves. On current battlefields we see a real spread of sophistication of these systems, from highly complex specialist robotic and automated systems developed for military use, to comparatively basic and cheap products readily available for purchase online.

Digital militaries create data. What began as simple messages, passed point to point has grown to become giant warehouses of data now widely available in a networked force. In my experience, I've witnessed that volume of data expands beyond what could ever be processed by humans, in a timely fashion anyway. The potential of early AI to improve data analysis and information processing led it to early roles in Command and Control (C2) functions, and perhaps also because the headquarters were the only locations with the processing power to support it. As algorithms have advanced, they have been used in the most advanced militaries to analyse vast amounts of data to help commanders make better decisions faster. Having been enabled to decide quickly where to strike, the lethal systems they employ have their own AI on board to increase accuracy and effect.

It's worth saying a word about autonomy I think and drawing a distinction with automation. Automation often still requires significant human intervention. Remotely controlled robots still have human operators, drones have pilots (although the burden of flying control has decreased). AI is taking us towards greater autonomy because the more the machine is learning for itself, the less human intervention is necessary. As part of this thinking about Human Machine Teaming (HMT) has grown rapidly. On operations in Iraq in 2016, the aviation teams were developing the TTPs for Manned Unmanned Machine Teaming (MUMT) using AH-64 teamed with UAVs where the UAV did the find and the AH did the strike. Integrating AI and robotics with human operators creates systems that leverage the strengths of both humans and machines.

Reflecting the widely acknowledged strategic importance of these technologies, I've seen an explosion of research and development in AI and robotics. Significant investment in developing, experimenting and trialling these capabilities, along with testing in operational environments, has led them to evolve Like many new technologies, there is much debate about the relative merits of cutting-edge military technology development programmes vs buying 'off the shelf' and modifying of making do. A well-known debate in the UAV/drone arena, where the use of online purchased quadcopters to drop a hand-grenade or mortar, while filming it for online information operations, has been a staple of the Russia-Ukraine War media feed.

**I have noted that use of robotics and AI also raises ethical questions, especially for liberal democracies. Who controls these systems, what failsafe should be in place, would an autonomous system have ability to decide on use of lethal force, what does that mean for accountability and the law of armed conflict?**

My overarching impression is that the integration of AI and robotics in the military is an ongoing process, one in which we are probably only at the very beginning. R&D and experimentation is revealing the art of the possible, but even the most sophisticated militaries on the planet are still only scratching the surface of potential from robotics, machine learning, autonomy and AI.

**Reflecting on your service, can you discuss the shift in emphasis on cybersecurity, the current challenges faced by today's military leaders?**

Military leaders now face significant challenges as they navigate increasingly complex and interconnected digital battlefields and operating environments. As cyber threats become more prevalent, persistent and sophisticated, military leaders have a new dimension to Force Protection to consider. A digital force equipped, organised and trained to exploit digital and connected systems to deliver its effects, is also vulnerable to attack that renders those systems ineffective or compromised.

So military leaders must ensure their systems are secure against state adversaries, who can use cyber-attack to operate below the threshold of war, violent non-state actors who can use the asymmetry of cyber to achieve disproportionate effect and even just malevolent hackers who seek to cause disruption. Adversaries are constantly evolving methods and tactics to bypass security measures, so effective defence of networks is a constant battle. The rules of engagement in cyberspace are not clear, and your adversary may not be operating to the same code of ethics as you. You may be limited by your policy leaders in how and what you can attack with offensive cyber, while your enemies may not.

And of course, it's not just the battlefield and combatants that are exposed. Supply chains, transport links and industrial bases are also vulnerable and, in many cases, not in the control or even purview of the military. A sophisticated cyber-attack on a supply chain could stop or redirect re-supply and diminish combat forces without a shot being fired. And the global supply chains we use to supply our equipment and systems introduces potential vulnerabilities if adversaries compromise them, leading to the inclusion of malicious components in military systems.

Military leaders do not always have access to the most skilled cybersecurity professionals which means they do not always have the workforce to address the challenges they face. Absent conscription it is challenging for militaries to attract and retain the best young technical minds when opportunities and rewards are greater elsewhere. Use of AI could help, with machines tasked with learning to identify and protect against attack. But the same is true for our adversaries who may be willing to use the power of AI to automate and enhance the effectiveness of their offensive cyber and dramatically scale up the intensity of cyber-attack on our systems.

So military leaders face a significant security challenge and with it a delicate balancing act between the need for connectivity and interoperability, and the imperative to maintain a high level of cybersecurity. An overemphasis on securing against a seemingly omnipotent and omnipresent threat, could limit a force to point of uselessness, but too little protection leaves it exposed and vulnerable. Addressing these challenges requires a comprehensive and adaptive approach, encompassing technology, policies, training, and international cooperation.

### Given the rapid advancements in AI and robotics, how do you believe military training and strategy development should adapt?

Adapting military training and strategy to advances in AI and robotics will require a holistic approach that considers technological, ethical, and wider political factors. Balancing innovation with responsible use is key to leveraging the benefits of these technologies while maintaining security from adversaries and political consent. Here are some of the areas I would focus on:

We must develop the Human-Machine Teaming. Increasing the collaboration between humans and machines is key, in every domain, across domains, and at every level of warfare. AI should be viewed as a tool to augment human capabilities, with humans maintaining ultimate control over critical decision-making processes.

Increase the use of AI for decision support. AI offers a powerful tool for processing vast amounts of data, providing real-time intelligence, and offering predictive analysis. Integrating them into C2 structures and processes can enhance decision-making capabilities and dramatically enhance speed of response, effectiveness of actions and create tempo and momentum in battle. It is also vital to build effective capability and train the force in peace.

Create dedicated Cyber and AI Forces. With the increasing importance of cyber and AI operations, defensive and offensive, military personnel need specialised training in cybersecurity and AI. New units, with the right personnel, skills and ethos are required rather than hoping existing organisations and structures can adapt or attract the right new people.

Focus on Interoperability and Collaboration. Allies must not do this in isolation. Despite the complex ethical, political and cultural differences they may have, military forces need to ensure that AI systems and robotic platforms are interoperable. Communication protocols, data formats, policies and tactics need to be aligned wherever possible. Exploit AI to improve training. It's not just about training in cyber and AI, which could be left to specialists initially, but just as important is using these technologies to better simulate realistic scenarios for the wider force, enhance decision-making skills, and provide adaptive training modules. Virtual Reality (VR) and Augmented Reality (AR) are already available and in use but could be used more widely and in a more connected way to create immersive training environments that mimic real-world conditions.

Militaries must be ready to counter the threats. As laid out above, this presents as much threat as opportunity.

Getting the cybersecurity defences in place, effective but not disproportionately impacting operational output is vital. This needs systems, skills and workforce, but there is a need to also develop policies and strategies. This is needed to guide the counters and responses to potential threats from adversarial AI systems, cyberattacks and misinformation. It is an area with significant ethical considerations, sometimes few guidelines due to the novel technologies involved, but public and political engagement is necessary to allow these critical aspects of military adaptation. Addressing concerns and building trust is essential for the acceptance of these technologies in society.

**From your vantage point, how crucial is international cooperation in establishing norms and standards for emerging technologies in defence?**

As I said earlier, international cooperation is one of the top priorities for focus and strategy around emerging technologies in Defence. The rapid advancement of artificial intelligence, robotics, cyber and autonomous systems, has led to a growing recognition of the need for shared endeavour, strategy, standards, rules and approaches to ensure successful, effective and ethical use. This is about both who you cooperate with and what you cooperate on.

Alliances such as NATO offer an obvious framework for multinational cooperation to develop these capabilities. They can provide the forum for strategy and policy alignment, but also the standardisation (STANAGs) necessary to allow systems to interoperate and the mechanisms for joint research initiatives. Meanwhile international fora, like the UN, have provided a platform for discussions on the use of emerging technologies in the context of international peace and security. The UN Office for Disarmament Affairs has a Group of Governmental Experts on Lethal Autonomous Weapons Systems which has led discussions on meaningful human control and the application to humanitarian law.

International cooperation needs to reach beyond the actions of large international bodies. Collaboration between governments and the private sector is also essential in establishing norms and standards. Engagement with industry, which is expanding to include new technology companies coming to the sector with their new AI, cyber and network products and capabilities, is also essential. Having earlier said that emerging technologies such as AI and cyber have exposed skills gaps, relationships with civil society through industry and academia are vital to advance and diversify thinking about novel technologies. If confidence is to build around the world that new technologies are being developed and used in alignment with the existing conventions of the international order, then more transparency and information sharing is needed. Transparency in military capabilities and intentions is crucial for building trust among nations. Discussions on ethical guidelines for the use of emerging technologies are integral to international cooperation. The more these include civil society organisations and experts, the more diverse and far reaching the cooperation will be. Therefore, the more likely it will be able to cover everything from norms and standard on the legal and ethical use of AI, autonomy and cyber as well as the effective collaborative use of these technologies.

**Throughout your service, can you recall a specific moment when the ethical challenges of deploying advanced technology in warfare became especially salient?**

Perhaps not specific, but I think back to my time on operations in Iraq and Afghanistan, and particularly the use of sophisticated systems as part of our targeting of key members of the terrorist networks in both theatres. While this was not a conflict that we would say employed autonomous or artificially intelligent systems, or indeed one in which we were fighting our adversary in the virtual domain or cyberspace, the use of semi-autonomous lethal systems and human machine teaming raises many of the ethical considerations that we've been discussing today.

In the targeting cycles that we operated in our Headquarters, considerations around collateral damage and risk to civilians, about accountability and responsibility, and with it who held responsibility for the use of lethal force and where on the battlefield they were. Many of the key aspects of the conversations we've been having today about the ethical use of even more advanced technologies were present in these previous operational experiences. I think about the targeting cycles and engagements and the extensive analysis and conversations (albeit often at great pace for fleeting targets) that took place about human control in these loops just as we're now having conversations about whether fully autonomous weapons have adequate human control. During those events, we discussed how control was retained once a long-range precision strike missile had been launched. We discussed how the human remained in the loop either to maintain positive identification of the target, or indeed to provide the commander with a terminal abort opportunity if they were no longer satisfied that the target was legitimate. In these discussions that I witnessed first-hand where humans were making ethical and proportional decisions based on a set of rules of engagement, required to differentiate between combatants and non-combatants. Then I find myself thinking about whether the most sophisticated AI systems would be better or worse than humans at this or indeed whether a computer would be better placed to do the legwork leaving only the final decision for the human.

It's the accountability and responsibility aspects of those experiences that I find most instructive to think about. Things go wrong in war, and just as autonomous systems could make mistakes, we know from experience that so do humans. In history some humans have been held accountable for their mistakes in war, some individuals for their mistakes in Iraq and Afghanistan. As machines are part of the decision action loop, and the more that artificially intelligent systems are making key decisions, the opaquer that accountability will become. Identifying 'who' is accountable when something goes wrong is going to be even harder than it was in the investigations and inquiries that followed mistakes in Iraq and Afghanistan.

**What advice would you offer to current defence leaders as they navigate the intricacies of weaving these technologies into their operations?**

I'm not sure I'm qualified to be advising anyone on these matters. There are some brilliant people much better placed to guide our Defences leaders on the intricacies of these most advanced technologies. But perhaps I can offer some thoughts on weaving technology into the force and onto operations, from experience, that is more generic than the specifics of AI, Cyber or autonomous systems that we've been focussing on today.

I think we can be bolder. Experiment of course, but have a plan to exploit what you find, know how to grow up the technology readiness ladder. Be willing to "buy to try" and place technology in the hands of the user. Be willing to take more risk on buying good enough and then evolving it in service. The more hi-tech the technology the greater the temptation to keep it in the test and evaluation arena but try to overcome that instinct whenever possible.

Pick partners rather than products. Finding, testing and buying the best technology products is nearly always a journey, so find some people you trust to travel with. The right international allies and industrial partners are essential to share risks, ideas, costs and work with. Not only will it likely allow faster progress, but it will also naturally create your cooperation and interoperation, increase standardisation and align policy and TTPs.

Expect resistance. It will be hard; things will go wrong, and most new technology starts out with more doubters than supporters because it makes people feel uneasy and out of control. All the myriad reasons not to pursue, to invest, to develop will be presented (it won't work, it's too dangerous, it's too expensive, don't be an early adopter etc), so be ready to test and challenge those perceptions and be ready to lead your organisation though the change.

View an in depth panel discussion
on Emerging Technologies

CLICK HERE

iDeaS
BY COGES EVENTS

Powered by

ABLO
CONSULTING