Making sure the adoption of

AI in cyber security remains ethical in Defence

The world is how we shape it

sopra steria

Introduction

The ethical issues of Artificial Intelligence (AI) have been widely explored over the last few years, with over 200 sets of ethical principles having been published. However, these often remain abstract and provide no guidance for operationalisation. This is a problem in all areas, but most prominently in cyber security where the impact of AI is being increasingly felt, particularly in defence and national security. From the 2016 Shadow Brokers cache coming from NSA and leading to the WannaCry attack on the NHS to the 2021 attack on the US Colonial pipeline, cyber attacks are increasingly impacting our critical infrastructure. This will only get worse as AI is further integrated into attack methods. Despite this, there is little guidance available for ethical responses to these challenges.

AI can be used in several ways in cyber security, both in offence and defence. It can be used to scrape information for spear phishing campaigns, or to develop disinformation using deep fakes to divide and manipulate opinion. It can be exploited to expose sensitive data used to train AI models and modify input to poison those models. The poor or inept use of AI can open further opportunities for attackers to exploit. Lastly, and more positively, AI can be used to develop mitigations against adversarial attacks through recognizing a typical behaviour and developing complex encryption.

In defence, AI applied to cyber security promises exciting opportunities. It can be an enabler, by providing situational awareness; it can provide resilience by helping to assure and secure sensitive information; it can provide denial to adversaries through deploying deceptive techniques; and it can be an effecter of capabilities through behavioural analytics. AI is therefore central to an information advantage strategy. By contrast, given the rise in AI use in offensive cyber operations against defence targets, there is no real alternative but to adopt it and meet the challenge head on.

With the complexity and scale of the problem, we might ask why we should worry about an ethical approach. Surely that would just tip the balance in favour of the "bad guys"? Shouldn't we acknowledge the cyber arms race and remain relevant rather than ethical?

Choosing the right response

There are two responses to this concern. Firstly, while security is important, it is not the only value of importance. In democracies we accept some costs which come with our civil freedoms, and the cost of some cyber-attacks may be included in that. We would not choose to live in a police state, even if that would guarantee our safety on the streets at night. Likewise, we recognise we should not target civilians in war, even when we believe that doing so might shorten that war.

Secondly, unethical responses get exposed. Whether through internal compliance audits, organisations being hacked, or disillusioned insiders such as Edward Snowden sharing information with the wider world, it is hard to keep unethical activity secret. When it is revealed the activity ends, and alternatives need to be found. Genuinely sustainable solutions therefore must be ethical.

So what are the ethical concerns regarding AI and cyber security? If we do not have a robust cyber security operation in defence to respond to attacks, then we face myriad risks against individuals and society. At the personal level, sensitive data may be uncovered and shared, deep fakes can destroy a person's reputation, IP may be lost, and we risk physical, financial, psychological and emotional harm. At the societal level, military and critical infrastructure may be harmed, as was the case when the Ukrainian power grid was taken down in 2015; there may be widespread physical harm, as with the WannaCry attack on the NHS in 2017; there are widespread privacy harms, directly impacting the low take up of the NHS track and trace app in 2020; there may be democratic consequences such as the Cambridge Analytica scandal in 2016; and there can be large scale financial harm as was felt in the recent US Colonial pipeline attack in 2021.

Investing in the right cyber security solution

These are the ethical reasons to invest in cyber security. However, there are also ethical reasons to be cautious as we do so. As noted above, there are widely recognised ethical concerns with AI in general, many of which apply to cyber security. Firstly, evidence used to arrive at decisions may be inconclusive, it may be inscrutable, or it may be misguided. These may each be exacerbated by the opaque nature by which some AI systems arrive at conclusions, and the problem of ***"automation bias",*** the tendency of people to trust automated systems even when they go against common sense. Secondly, these can then impact outcomes which may be unfair, untraceable, and even transformative of behaviour. Thirdly, a failure to anticipate and address these concerns will undermine the sustainability of the response. This will have an impact on civil-military co-operation, compliance, and recruitment and retention of staff.

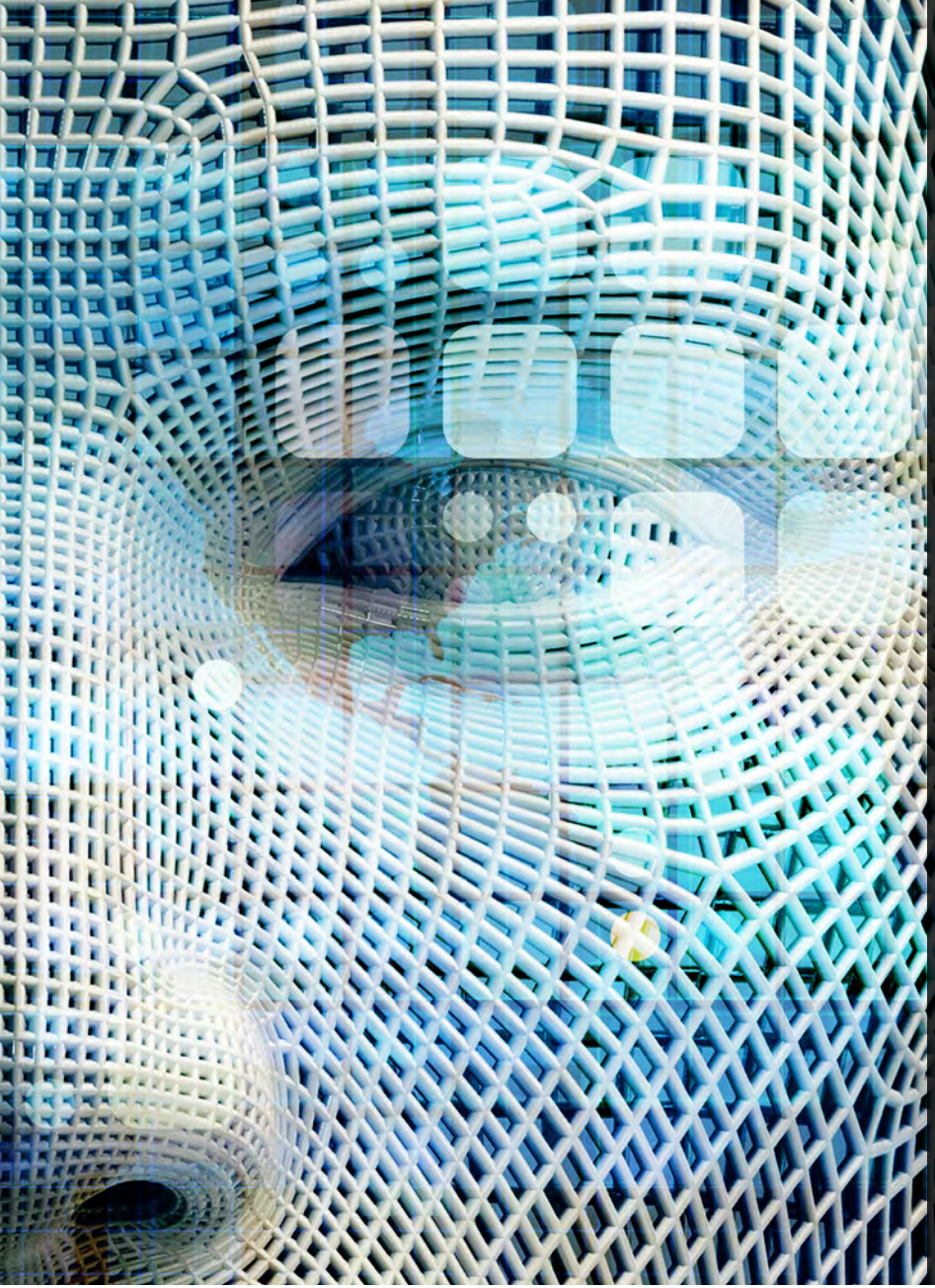
As technology adoption is already rapidly outpacing policy we believe there is a rapidly building case for MOD to consider some fundamental questions:

1. Is the application of AI an area that MOD wishes to actively shape and guide or leave open loop?
2. Do the risks and concerns need some sort of policy, compliance or assurance response?
3. If so, who might own it?

And

4. Are the right handrails and guardrails in place to guide solution development and technology adoption?

In conclusion, there is no real option other than to apply AI in cyber security to meet the increasing complexity of attacks. Information advantage cannot be captured or maintained without it. While it may be appealing to ignore or sidestep ethical concerns to compete in the cyber arms race, doing so will undermine the long-terms sustainability of solutions. This leaves the question as to whether the guardrails are in place in defence and beyond to ensure that the adoption of AI in cyber security is and remains ethical.



More Information

To help organisations answer the key questions raised in this article Sopra Steria has a world class cyber security group, providing a range of options to clients from education and vulnerability awareness to developed penetration testing. We are also unique in having a dedicated and highly successful digital ethics team with expertise in AI and cyber security ethics.

For more information on our AI and Security services for Defence and Government organisations please contact one of our specialists below who will be happy to help you.

Dr. Kevin Macnish
Digital Ethics Consulting Manager
E: kevin.macnish@soprasteria.com

Dr. Peter Bruce
Head of ADS Consultancy
E: peter.bruce@soprasteria.com

Or you can visit us at https://www.soprasteria.co.uk/industries/defence

We look forward to working with you.

The world is how we shape it

sopra steria