Policinginsight

ANALYSIS:

Enhancing cyber security: The use of artificial intelligence

3rd November 2021 | Andrew Staniforth | Policing Insight

Picture © Traitov / iStockphoto

With the site of a new National Cyber Force now confirmed – along with the centre's role in "offensive cyber operations" – the UK has reinforced its position as a leading player in global cyber security; Policing Insight's Andrew Staniforth looks at plans for the NCF, the country's continuing efforts to build cyber capacity, and the opportunities for developing new uses of artificial intelligence within those disruptive technologies.

Last month it was confirmed that the UK's new National Cyber Force (NCF) – announced by the Prime Minister as part of the Integrated Review in November 2020 – will establish its £5billion campus in the village of Samlesbury, near Preston in Lancashire.

> "The MoD said the NCF will be working 'in partnership with law enforcement and international partners', and will operate 'in a legal, ethical and proportionate way to help defend the nation and counter the full range of national security threats'."

The NCF will draw together personnel from intelligence, cyber and security agency Government Communication Headquarters (GCHQ), the Ministry of Defence (MoD),the Secret Intelligence Service (MI6)and the Defence Science and Technology Laboratory (DSTL), under one unified command for the first time.

The decision cements the North-West of England's position as the cyber centre of the UK; GCHQ has an office in Manchester, and the city is Europe's fastest growing major tech cluster, with more than 15% of Manchester's population employed by the digital, creative and technology sector. Salmesbury is also already home to an aircraft factory for aerospace defence company BAE Systems.

Defence Secretary Ben Wallace said the NCF will create "thousands of highly skilled jobs", and will play a lead role in the UK's offensive cyber operations – activities that can disrupt the efforts of hostile states, terrorists and criminals who threaten the UK's national security – from countering terror plots to conducting military operations.

The MoD said the NCF will be working "in partnership with law enforcement and international partners", and will operate "in a legal, ethical and proportionate way to help defend the nation and counter the full range of national security threats".

Capacity building

The creation of the NCF (a separate entity to the National Cyber Security Centre (NCSC)established in 2016) extends the UK's global leadership on offensive cyber operations, with GCHQ pioneering the use and development of these cyber techniques.

In 2016 the then Defence Secretary Sir Michael Fallon confirmed the UK was conducting cyber operations against Daesh, and in 2018, GCHQ Director Jeremy Fleming revealed how it had degraded ISIS propaganda networks through cyber operations.

> "For many years security policymakers and defence experts have been concerned about the increasing regularity and aggressive nature of hostile cyber-attacks."

The UK was also the first country to offer these cyber capabilities to NATO; now, through the NCF, these will be an increasingly important contribution to that alliance.

Building cyber capacity to protect the UK remains an important part of both national defence policies and national security strategies. For many years security policymakers and defence experts have been concerned about the increasing regularity and aggressive nature of hostile cyber-attacks, suggesting that a new security apparatus and architecture needed to be developed to keep pace with new and emerging threats.

The creation of the NCF provides strong evidence that this new architecture is nearing completion. Building capacity to deter and detect cyber threats, as well as investing in new cyber capabilities, has presented a challenge to many nations across the world.

In Europe, major investments in developing cyber capabilities have also been made over recent years, including the creation of Europol's European Cybercrime Centre (EC3) in 2013, to co-ordinate cross-border law enforcement activities against computer crime and act as a centre of technical expertise.

The creation of EC3 strengthened Europe's response to cybercrime, complementing the European Union Agency for Cybersecurity (ENISA) founded in 2004.

Disruptive technologies

The European Commission, following representation from Europol and EU member states intelligence and law enforcement agencies, continues to invest in new cyber security research and innovation programmes to enable the next generation of cyber defence tools, techniques and technologies to be developed.

Under Cluster 3: Civil security for society of the Horizon Europe innovation programme, the European Commission Research Executive Agency has made €11million available this year for research projects to examine and explore the use of artificial intelligence (AI) for cyber security reinforcement.

> "This research call provides an excellent opportunity for assets of the UK's new cyber security machinery – as well as police cybercrime units – o engage in ground-breaking research and innovation activity with EU partners."

Proposals for three-year projects are now being invited from public, private and academic partners across Europe to propose actions which develop AI-based methods and tools in order to improve system robustness, resilience and response to cyber attacks, as well countering the ways AI can be used for attacking.

Advanced AI-based solutions, including machine learning tools, as well as defensive mechanisms to ensure data integrity are also encouraged to be included in the proposed actions for grant-funding.

The expected outcomes of the projects must serve to reinforce cyber security using AI technological components and tools in line with relevant EU policy, legal and ethical requirements, as well as increasing the knowledge about how an attacker might use AI technology in order to attack IT systems.

As the UK remains eligible for Horizon Europe grant funding, this research call provides an excellent opportunity for assets of the UK's new cyber security machinery – as well as police cybercrime units – to engage in ground-breaking research and innovation activity with EU partners.

Active participation and engagement in a project under this call will provide cyber security operatives with an insight into future cyber security challenges, and most importantly, provide an excellent opportunity to inform the development of new tools and techniques, serving to harness the capability of AI for both defensive and offensive cyber operations.

Link to online article at Policing Insight: https://policinginsight.com/features/enhancing-cyber-security-the-use-of-artificial-intelligence/

Andrew Staniforth is Director of Innovation at SAHER (Europe), a security research, training and consultancy operating at a global level, participating in the NOTIONES (*iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS*) network, funded by the European Commission Horizon 2020 Programme (No. 101021853). Andrew is also an active Researcher of Cyber Threats at the Hillary Rodham Clinton School of Law and Criminology, University of Swansea. As a former Counter-Terrorism Detective, he has worked across the world and supported missions of the United Nations Terrorism Prevention Branch. **Contact:** Andy@saher-eu.com
To learn more about NOTIONES visit: https://www.notiones.eu