MODULE SPECIFICATION

Module Title:	Digital Policing and Counter Terrorism	**Level**:	5	**Credit Value**:	20

Module code:	POL504	**Is this a new module?**	No	**Code of module being replaced**:	N/A

Cost Centre:	GACJ	**JACS3 code**: HECOS Code:	L611 100484

Trimester(s) in which to be offered:	2	**With effect from:**	September 2019

Faculty:	Social and Life Sciences	**Module Leader:**	Andrew Crawford

Scheduled learning and teaching hours	30hrs
Guided independent study	170hrs
Placement	0hrs
Module duration (total hours)	200hrs

Programme(s) in which to be offered	Core	Option
BSc (Hons) Professional Policing	✓	

Pre-requisites
None

Office use only

Initial approval January 19

APSC approval of modification January 21 — Version 3

1. Jan 21 updates made to COP standards numbering and syllabus points
2. Jan 22 minor changes to syllabus and standards numbering as per COP requirements

Yes ☐ No ☐

Have any derogations received SQC approval?

Module Aims
To explore the nature of, and policing response to, Digital Policing and Counter Terrorism

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Understand the prevalence of technology and devices in modern society, their effect on policing and the personal and organisational risks associated with using them (NPC mapping Digital policing : 1.1,2.1,3.1.4,2.1,2.2,2.3)	KS1	KS4
		KS6	KS9
2	Examine how technology may be used in everyday policing (NPC mapping: Digital Policing: 3.1,3.2)	KS1	KS4
		KS6	KS9
3	Examine common and complex types of digital-facilitated crimes , the individuals who may be especially vulnerable and the impact of such crimes on individuals, businesses and families (NPC mapping: Digital policing: 4.1,4.2, 5.1, 5.2)	KS1	KS4
		KS6	KS9
4	Understand key counter-terrorism terminology/concepts and the organisational structures and inter-relationships that exist in counter-terrorism policing including their role/functions in past and present counter-terrorism operations (NPC mapping: Counter Terrorism:1.1,1.6,1.2,1.3,1.4,1.5,2.1,2.2,2.3,2.4,2.5,2.6,2.7,2.8,4.1,4.2)	KS1	KS4
		KS6	KS9
5	Analyse the potential links between terrorism and other forms of criminality and the role of policing in gathering intelligence relevant to counter-terrorism policing (NPC mapping: Counter Terrorism:,5.1,5.2,6.1)	KS1	KS4
		KS6	KS9

6	Understand key legislation relevant to counter-terrorism policing (NPC mapping: Counter Terrorism 3.1,3.2,4.1,4.2)	KS1	KS6

Transferable/key skills and other attributes
Independent working Presentation Group working Independent Working Time Management

Derogations
Module cannot be condoned/compensated on BSc (Hons) Professional Policing All elements must be passed on BSc (Hons) Professional Policing

Assessment:

There are 2 assessments for this module:

Presentation: In groups (n=4) Title: 'Digital Crime-Digital Policing'. 'Digital Crime section': students will explore the history of two forms of digital crime (one common (10 mins)/one complex (10mins)), the impact it has, and authority under which, and how, police might respond. Digital Policing section: Students to illustrate how technology may be used in everyday policing (10 mins) (followed by 10 mins questions)

Case study requires students to devise a police counter-terrorism plan in the case of a prolific offender now a prison leaver who has been radicalised in custody and soon to be released.

Assessment guidance will be provided that directs students towards meeting the relevant learning outcomes

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1-3	Group Presentation (individual marks awarded)	50%	40 minutes	
2	4-6	Case study	50%		2,000 words

Learning and Teaching Strategies:
The module will be taught online using a variety of strategies: wrap around lecture content, panopto videos, links to website and information, online exercises and discussions (a-synchronous). The module will be supported by two face to face seminars.

Syllabus outline: NPC Indicative Content Mapping

LO1: Understand the prevalence of technology and devices in modern society, their effect on policing and the personal and organisational risks associated with using them

Changing world of devices and device capabilities:

- Wearables (e.g. fitbits, apple watches etc.)
- GPS, satnav, drones
- Vehicle data (telematics, infotainment etc.)
- Internet of things (connected home)
- Games consoles (e-readers, other mobile devices)
- Routers, Wi-Fi, VPN and communications data
- Data storage, including Cloud, removable drives, memory sticks and volatile data

Common IT terminology associated with devices:

- Internet addresses (e.g. IP addresses, MAC addresses, mobile internet etc.)
- Email
- Social networking (e.g. social media, instant messaging)
- Mobile apps
- Source code
- Cryptocurrency
- Dark web, deep web

Supporting technology and how these support device functionality

- Social networks
- Apps and encrypted communications

Influences of technology and devices in a policing context

- First point of contact, social media etc.
- Digital witnesses (Echo, Google home etc.), CCTV, digital devices etc
- . • Investigative opportunities (CPIA 1996, investigative mindset)
- Community engagement

How to manage the security risk to self, and family:

- Keeping private life separate from work life and work identity
- Risk of being traced through technology, location service data etc.
- Social media association

What is meant by the term ‘digital hygiene’:

- Impacts of using personal devices for police business (e.g. automatic connection to networks, taking photographs etc.)
- Seizure of the personal device for evidence and subsequent disclosure at court (e.g. crime scene photographs)
- Risk of disclosure of personal data in court (if the device is seized)
- Risk of leaking information about live police operations
- Tracking and scanning devices

Key legislation applicable to ensure compliance and mitigate organisational risk when dealing with devices in a policing context:

- Computer Misuse Act 1990
- Wireless Telegraphy Act 2006
- Criminal Justice and Police Act 2001
- Investigatory Powers Act 2016
- Regulation of Investigatory Powers Act 2000
- Police and Criminal Evidence Act 1984
- Criminal Procedure and Investigations Act 1996
- ACPO Principles of Computer Based Digital Evidence 2012
- Data Protection Act 2018/General Data Protection Regulation (EU 2016/679 (GDPR) 2018

LO2: Examine how technology may be used in everyday policing

How digital technology may be used to assist with:

- Community engagement
- Managing incidents (instant messaging, public appeals for information etc.)
- Enhancing a criminal investigation (device location, attribution etc.)
- Enhancing communications

Considerations in the use of technology within policing:

- Legal restrictions on investigatory use of technology
- Digital footprint, personal and work devices
- Professional standards
- Disclosure considerations

Considerations associated with unlawful research/examination of a device, including assuming a fake persona

LO3: Examine common and complex types of digital-facilitated crimes , the individuals who may be especially vulnerable and the impact of such crimes on individuals, businesses and families

Common internet-facilitated crimes:

- Hate crime
- Extortion (e.g. sexting/revenge porn etc.)
- Abuse, bullying, stalking and threats or harassment
- Online fraud/cybercrime
- Child sexual exploitation
- Radicalisation
- Financial crime
- Modern slavery and human trafficking

Individuals who may be more vulnerable to digital-facilitated crimes e.g children, elderly, vulnerable adults

How criminals engage in complex internet-dependent crimes and the impact of such criminality:

- Hacking

- Malware
- Phishing
- Denial of service
- Browser hi-jacking
- Ransomware
- Data manipulation
- Cryptocurrency and cryptolocker offences

Impact of complex digital-related crimes on individuals and businesses

LO4: Understand key counter-terrorism terminology/concepts and the organisational structures and inter-relationships that exist in counter-terrorism policing

Radicalisation
Extremism, including Right Wing Terrorism (RWT) and Left Anarchist or Single Issue Terrorism (LASIT), Northern Ireland Related Terrorism (NIRT) and Islamist Terrorism (IT)
Interventions
Terrorism-related offences
CONTEST strategy: Pursue, Prevent, Protect and Prepare
Terminology and threshold matrix
National Counter Terrorism Policing HQ (NCTPHQ)
National Counter Terrorism Policing Operations Centre (NCTPOC)
Counter Terrorism Command (CTC)
Counter Terrorism Unit (CTU)
Counter Terrorism Intelligence Unit (CTIU)
Special Branch
Security Service
National Counter Terrorism Security Office (NaCTSO)

LO5: Analyse the potential links between terrorism and other forms of criminality and the role of policing in gathering intelligence relevant to counter-terrorism policing

Intelligence in counter-terrorism operations:

- Local
- Regional
- National

Importance of community intelligence in counter-terrorism operations:

- Community engagement
- Developing intelligence
- Fostering co-operation

LO6:Understand key legislation relevant to counter-terrorism policing

Methods of funding/enabling terrorism, including:

- Money laundering
- Fraud
- Identity theft

Bibliography:

Essential reading

- Taylor, R.W., Fritsch, E.J. and Liederbach, J., (2014). Digital Crime and Digital Terrorism. Prentice Hall Press.

Digital Policing.

- Bryant, R. ed., 2016. Policing digital crime. Routledge.
- College of Policing(2018) Digital Investigation and Intelligence Authorised Professional Practice https://www.app.college.police.uk/app-content/digital-investigation-and-intelligence/?s=
- Gillespie, A (2015) Cybercrime: Key Issues and Debates. London: Routledge
- Hitchcock, A., Holmes, R. and Sundorph, E., 2017. Bobbies on the net: a police workforce for the digital age.
- HMIC (2015) Real Livers, real crime: A study of digital crime and policing. London:HMIC https://www.justiceinspectorates.gov.uk/hmicfrs/?cat=digital&force=&frs=&year=&s=&type=publications
- McMurdie, C., 2016. The cybercrime landscape and our policing response. Journal of Cyber Policy, 1(1), pp.85-93.
- Richardson, L., Beadle-Brown, J., Bradshaw, J., Guest, C., Malovic, A. and Himmerich, J., 2016. "I felt that I deserved it"–experiences and implications of disability hate crime. Tizard Learning Disability Review, 21(2), pp.80-88.
- Wall,D.S and Williams,M (2014) Policing Cybercrime: Networked and Social media technologies and the Challenges for Policing

Police Counter Terrorism

- Hutton,G.,Mckinnon,G and Connor,P (2018) Blackstone's Police Manuals Volume 4: General Police Duties 2019 Chapter 4.9 Terrorism and Associated Offences. London: Blackstone
- Joyce,P (2016) The Policing of Protest, Disorder and International Terrorism in the UK since 1945. London:Palgrave/Macmillan.
- McMurdie, C., 2016. The cybercrime landscape and our policing response. Journal of Cyber Policy, 1(1), pp.85-93.
- Murphy, K., Madon, N.S. and Cherney, A., 2017. Promoting Muslims' cooperation with police in counter-terrorism: The interaction between procedural justice, police legitimacy and law legitimacy. Policing: An International Journal, 40(3), pp.544-559.
- Staniforth, A (2013) Blackstone's Counter-Terrorism Handbook. London: Blackstone Or
- Silke, A. ed., 2018. Routledge Handbook of Terrorism and Counterterrorism. Routledge.

Other indicative reading

Digital Policing

- Broadhurst, R, Grabosky, P, Alazab, M and Chon, S (2014) Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology Vol 8 Issue 1: 1-20..
- Gilmour, S., 2014. Policing crime and terrorism in cyberspace: An overview. European Review of Organised Crime, 1(1), pp.143-159
- Horsman, G., 2017. Can we continue to effectively police digital crime?. Science & Justice, 5 Jones, C., 2015. Managing extremist offenders: The TACT-ics of policing thought?. Probation Journal, 62(2), pp.172-180.7(6), pp.448-454.
- Loveday, B., 2017. Still plodding along? The police response to the changing profile of crime in England and Wales. International Journal of Police Science & Management, 19(2), pp.101-109.
  Gannoni, A., Willis, M., Taylor, E. and Lee, M., 2017. Surveillance technologies and crime control: understanding police detainees' perspectives on police body-worn video (BWV) and CCTV cameras.

Police Counter Terrorism

- Blakemore, B., 2016. Policing cyber hate, cyber threats and cyber terrorism. Routledge.
- Blakemore, B., 2016. Extremism, Counter-terrorism and Policing. Routledge.
- Dunn, K.M., Atie, R., Kennedy, M., Ali, J.A., O'Reilly, J. and Rogerson, L., 2016. Can you use community policing for counter terrorism? Evidence from NSW, Australia. Police Practice and Research, 17(3), pp.196-211.
- Innes, M., Roberts, C. and Lowe, T., 2017. A Disruptive Influence?"Prevent-ing" Problems and Countering Violent Extremism Policy in Practice. Law & Society Review, 51(2), pp.252-281.
- Thomas, P., 2016. Youth, terrorism and education: Britain's Prevent programme. International Journal of Lifelong Education, 35(2), pp.171-187.
- Ragazzi, F., 2016. Suspect community or suspect category? The impact of counter-terrorism as 'policed multiculturalism'. Journal of Ethnic and Migration Studies, 42(5), pp.724-741.
- Silke, A. ed., 2014. Prisons, terrorism and extremism: Critical issues in management, radicalisation and reform. Routledge.