SudoCyber

Tactical Cyber Capability Development

"Teach your troops to hack correctly
because being good at
Red Team
makes them great at
Blue Team"

Brigadier, British Army

'Delivered by
5th Domain Operators
for 5th Domain Operators'

Skills development, by military people, for military people

SudoCyber

BLUF: Bottom Line Up Front…

False flags, disinformation and proxy actors have made attribution of cyber-warfare slow and uncertain. Wildcat cyber activity by partially trained operators within our armed forces could unwittingly cause geopolitical complications or even prompt military retaliation in some sensitive theatres. The logical policy is to escalate decision-making about cyber-operations to strategic command level. However, this translates into an unintended 'ban' on cyber-activity at a tactical level. Our troops are training, exercising and operating in urban environments without realizing they are surrounded by internet-connected access points and devices, all of which can be used against them – scanned, tracked, targeted, misguided, sabotaged and out-manoeuvred by cyber-tactics, techniques and tools that they know little or nothing about and are ill-equipped to defend themselves against - **they deserve our help!**

New Urban Warfare Threats

Teaching troops how to Hack

Blending cyber tactics into Battlecraft syllabus

Ex CAMBRIAN PATROL, the British Army's toughest patrolling event, 9 tests across 60km, with 40kg in 2 days. Tanks, crashed helicopters, medivacs, night attacks, river crossings, drones and now, cyber attacks! Capture-the-Flag exercises, run parallel to patrols, link the OpInt chain from handing in a laptop found in a building-clearance to hacking the laptop then passing intel back to the patrols helping their tests. End-to-end **multi-domain interoperability**

Red Team content

1. Cyber Intelligence Briefing
2. Passive & Active Reconnaissance
3. Weaponization of Code
4. Delivery Methodologies
5. Exploitation of Vulnerabilities
6. Establishing Command & Control
7. Actions On – Damage Control

Blue Team content

8. Threats in Urban Environments
9. Vulnerabilities in Equipment

Gamified learning to encourage competition

The SudoCyber platform is a SaaS-based gamified system, designed by serving military people, specifically to help develop cyber capability in the armed forces. **Ex-SF, Royal Marine and SigInt** operators are able to deliver complex cyber content in military context, speaking from their own experiences. The platform has restricted access that enables classified and hardware-specific content to be delivered and managed securely.

Learn, practice anytime, anywhere

A range of courses, with qualifications from **CompTIA** and the **EC-Council**'s Certified Ethical Hacking, complimented by 1,000+ labs and challenges in a Cyber Range that can be filtered by difficulty, topic and technique, are supported by Streams of labs on popular skills like Crypto, AI & OSINT. Accessible through a browser, troops can learn and develop new skills, at their own pace, in their own time, on exercise or on deployment.

Ongoing, integrated training to accelerate military capability development in tactical cyber

Concept Briefings

Introductions to the true nature of the 5th Domain of warfare. From nation-state efforts to tactical cyber threats, the briefing will raise awareness of the tools and techniques used in cyber activity and motivate troops to learn more about hybrid warfare.

Training Courses

3-5 day practical courses, for groups of 6-8, on camp or at our custom-built secure training facilities. With on-site test center, where candidates can be taught and certified at the same time. Practical hybrid learning sessions using the SudoCyber platform as a teaching aid which troops can continue using after the course ends.

Continuation Training

To reinforce the learning and to prevent skills fade, troops will retain their licenses to use the platform. This enables your commanders to organize follow-on activities, to keep the subject alive and SudoCyber personnel can assist on-site or remotely by running short sessions, CTF events and practical tutorials involving equipment such as drones, scanners, handheld devices and hacking tools.

Battlecraft Exercises

All teaching staff are either still serving or veterans and they are DV security cleared. This means that they are able to take part in training and/or exercises to help with multi-domain integration of cyber activities into the ITRs or Battlecraft syllabus. This work will obviously be dependent on gaining assurance, as well as the appropriate sign-offs, from appropriate chains of command and exercise leads.

Pre-Deployment Training

As with all complex technical subjects, especially those involving sensitive equipment such as radios, computers and others comms kit, it is critical that troops receive refresher training prior to being deployed to theatres where they will be required to be current and competent SQEPs. Tailored Streams of Labs can be assembled, which troops can complete on the SudoCyber platform, at their own pace, or as a short session delivered during their pre-deployment training activity.

Specialist Skills Development

Suitably motivated troops developing additional specialist skills is good for the individual, good for the unit and good for overall retention. Of all the subjects that are available for troops to volunteer to become more skilled at, cyber ranks amongst the most current, topical and important. For a special operations forces unit, or any active combat unit, having a cyber SQEP embedded in the front-line organisation is incredibly valuable, SudoCyber makes this possible.