



THE DEFENCE FORCES MAGAZINE

AN COSANTÓIR

www.dfmagazine.ie

(ESTABLISHED 1940)

Price: €3.00 (Stg £2.70)



DEC 2018 / JAN 2019

'VISORS DOWN'

CROWD RIOT CONTROL

[STRENGTHEN THE NATION]

ISSN 0010-9460



84

9 770010 946001

Building Our Awareness to CYBER SECURITY

BY DINOS ANTHONY KERIGAN-KYROU

Everyone in the Defence Forces operates in cyberspace - the environment in which all electronic communication takes place. We use it for our personal lives. And we increasingly use it within the military. And the cyberspace for both is interlinked. Cyber security is the security of everything we do in cyberspace.



What we do online - social media, messages, photos, videos we post - has potential security implications for ourselves and the Defence Forces. Likewise, equipment we use in the in the Army, Air Corps, and Naval Service - and across the EU within PESCO - is increasingly connected online using sensors, actuators, and control systems: the military 'Internet of Things' (IoT). Indeed, our critical infrastructure - such as our transport and energy supply - increasingly comprises IoT.

All this activity takes place in one shared cyberspace. There's no separate or 'secure' internet for 'important stuff' such as defence and critical infrastructure, and another one for posting Facebook photos, shopping on Amazon, and watching Netflix. There is only the one internet.

Information about you online is valuable to nefarious actors. They could be criminals after your money. Or blackmailers wanting to exploit you. It might be hostile states spying on Ireland. It could be someone trying to access your phone's camera or microphone - turning the device into a bug you'll be totally unaware of. It could be someone looking for information about Defence Forces equipment, or seeking to remotely control our weapons systems. It could be a terrorist seeking information about your barracks or the location and physical access details of your base on overseas deployment. Or they might want information about our UN, NATO, and EU partners. The list of motivation for breaching Defence Forces cyber security is endless.

The primary challenge is getting over the false concept that cyber security is all a technical matter. Cyber security concerns every single member of the Defence Forces. Over 80% of cyber security breaches are caused by organisational factors - not by some tech expert using complex code.

Indeed, there are two types of cyber security breach. Those you know of and those you don't. Demands for money, threats, cyber bullying, extortion and blackmail are overt threats. But you might also be compromised unknowingly. A nefarious actor or group may be able to monitor everything in your phone or computer. Connected military equipment can be compromised and moni-

tored over long periods without anyone knowing. They may see the location of your GPS and Armoured Personnel Carrier, or potentially compromise the multiple connected systems aboard an Offshore Patrol Vessel.

Watch out for anything unusual. Is your system slower than normal? Has information unintentionally changed? Have you clicked a link which might be suspect? Militaries worldwide don't really encourage questioning of senior ranks. However, "Was that email with the link actually from you sergeant?" could be a key question preventing a major security failure, potentially risking the lives of Defence Forces personnel. It takes just one such 'phishing' email to breach an entire system.

If you notice anything report it as soon as you can to CIS Helpdesk or via the IKON portal. Cyber threats, blackmail, or cyber stalking should always be reported to your Commanding Officer. CIS Corps is one of the most advanced information corps in the world and able to address any problem. You'll never be blamed for highlighting concerns - even if you think it resulted from your own error. And a cyber security problem identified early can be dealt with when it's small before becoming big. Your own cyber security - and the security of the Defence Forces - are intrinsically linked.

Next Issue: The online scams and threats that can endanger the security of you, your family, and the Defence Forces - and what you can do.



Dinos Anthony Kerigan-Kyrou coordinates and instructs on the 1st Joint Command & Staff Course, cyber security module. He is an instructor on NATO's DEEP - Defence Education Enhancement Programme - and is a co-author of the NATO / Partnership for Peace Consortium Cyber Security Curriculum.