



## Cyber Space

Professor Dr Reza Ziarati (C4FF)

Dr Lakhvir Singh (C4FF)

A wide range of hostile actors use cyber space to target the UK. They include foreign states, criminals, "hactivist" groups and terrorists. The resources and capabilities of such actors vary. Foreign states are generally equipped to conduct the most damaging cyber espionage and computer network attacks. Hostile actors conducting cyber espionage can target the government, military, business and individuals. They use computer networks, for example, to steal large volumes of sensitive data undetected. This might include intellectual property, research and development projects, strategic data on a company's merger and acquisition plans, or any other information that the owner might want to protect.

The risk of industrial cyber espionage, in which one company makes active attacks on another, through cyberspace, to acquire high value information is also very real. Cyber terrorism presents challenges for the future. We have to be prepared for terrorists seeking to take advantage of our increasing internet dependency to attack or disable key systems.

In countering cyber espionage and attacks Centre for Factories of the Future (C4FF) has developed a full degree programme and various modules have already been tested at associated universities including C4FF's own university, University Centre Garden City (UCGC). Furthermore, C4FF has started a new project named Cyber Spare to help mainly very small businesses to cope with complexity of computer systems and networks and become cyber security safe.

In parallel C4FF with support from several other organisation has become involved in a project which will deliver an encrypted traffic analysis service platform for cyber security. The platform will support a number of basic building blocks necessary for any Machine Learning (ML) and Deep Learning (DL) based traffic analysis. C4FF is pleased to be involved in this interesting and innovative project and disseminate and exploit the project outcomes in its network in UK and across Europe.

C4FF is an SME with RTD capacity based in Coventry and Kenilworth (UK). C4FF is the instigator of the Factories of the Future projects in the UK and supported similar developments in the EU. Since the company was founded in 1996, C4FF has gained extensive experience in participating and co-ordinating EU and UK funded R&TD projects in areas such as: Artificial Intelligence Systems, Cyber Security, Sales Forecasting, Market Intelligence Knowledge Extraction, Innovation Management, Factory automation and Enterprise Resource Planning. C4FF has several ICT, manufacturing facilities and laboratories worldwide. These laboratories are equipped with most up-to-date facilities. We also have access to several laboratories in several

partner institutions. C4FF has an established reputation for developing novel manufacturing systems and software for factory management, including for lean practices. We also have many years of experience in ICT and Manufacturing research and development, as well as cyber security. Cyber Security is of particular interest to C4FF Maritime Division supporting the shipping industry against cyber-attacks. C4FF has been involved in several EUREKA projects and currently support two ITEA3 projects.

The new research project now called ENTA will commence shortly. C4FF will use to support its local Cyber Space project and ensure small companies in its locality would also benefit from this research work.

ENTNA has already been approved and Cyber Space is also expected to be approved by the UK Government soon.