Not for general release in its entirety – Editorial background only

National Cyber Deception Laboratory
cyberdeception.org.uk

NCDL Inaugural Address 6th November 2019 at the National Cyber Deception Symposium, Defence Academy of the United Kingdom. Shrivenham Wiltshire. UK

Darren Lawrence
Director of the National Cyber Deception Laboratory

In 1940 Col Colin Gubbins was tasked by Churchill to prepare to defend against the expected Nazi invasion of the United Kingdom. Gubbins was not a specialist in building fortifications, like France's Maginot Line. He was not a commander who was known for directing large scale battle formations.

At that time of our war for survival, the unprecedented tactics of the mechanised Nazi Blitzkrieg were so effective in mainland Europe that the defence of our home was to be undertaken differently. Desperation required an unorthodox plan to stave off complete defeat.

Gubbins was an expert in Guerrilla warfare.

He oversaw the formation of the guerrilla force known as the Auxiliary Units. These irregular fighters drawn from local communities would not participate in the conventional defence of their towns and villages. Instead, their role started once the traditional attempts at defence had been inevitably overrun. The Auxiliary Units' purpose was to inflict maximum mayhem and

disruption over a brief but intensely violent period. Service in the Auxiliary Units was expected to be highly dangerous, with a projected life expectancy of just twelve days for its members.

How would this brutal plan for national survival fit with today's cyber-enabled world? Where defence challenges are played out in the intricate engineering of networks and the complex data science of the digital traffic they facilitate.

The issues then and now concern an active front in a war for our home territory.

General Sir Nick Carter, the Chief of the Defence Staff, has said that Britain is "at war every day" due to constant cyberattacks from Russia and elsewhere.
Distinctions between peace and war "don't exist any longer" in the modern world, has warned.
Speaking at the Cliveden Literary Festival, the head of the armed forces stressed that it is no longer possible to draw a clear line between competition and conflict.
"The changing character of warfare has exposed the distinctions that don't exist any longer between peace and war," General Carter said.
"I feel I am now at war, but it's not a war in the way we would have defined it in the past."

Taken from a Daily Telegraph article 29/09/19

Fighting an enemy on home soil stirs the most fundamental aspects of our survival instinct - even today, as a society we see the aggressive defence of our homes as being so legitimate, that the use of violence to do so is legally possible.

What about fighting for, and on our home networks? What commonalities can we find in the historical account of national survival using the guerrilla Auxiliary Units and the current battles of cyber defence?

- The need to defend against the unprecedented
- The reality of likely defeat in our defence of our home territory
- The need to change the rules of combat and face the costs and sacrifices that cannot be avoided in our attempts to fight back **within our home territory**

The need to defend against the unprecedented

The Chief of Defence Staff argues that the British military is facing new operational realities whose mechanisms and effects cannot be grasped with existing models and assumptions - yet old operational realities have not vanished! We still have combatant versus combatant. In combination, these conditions constitute a new form of an adversarial relationship. A relationship involving novel aims and mechanisms, where even the fundamentals of time and space are no longer straightforward. For example, are cyber attacks to be understood as discreet missile attacks between physically separated physical entities? Or are they a perpetual set of intimate knife fights between the digital proxies of the combatants? If it is the latter, then the operational challenges have more in common with the nightmares of a zombie apocalypse than they do with the mechanised Blitzkrieg of WWII

The reality of likely defeat in our defence of our home territory

A difficult question for us to consider is, have we lost our next war for national survival before a shot has been fired? This would be the case, if we had already lost the battle for the home territory of our information networks. Broadly speaking, if our systems are overrun, we would have no rear area from which to supply and control our digitally dependent weapon platforms - we would be fighting in enemy-occupied home territory from the very outset.

The need to change the rules of combat and face the costs and sacrifices that cannot be avoided in our attempts to fight back within our own home territory

There is one essential priority for both our discussion today and the intended role of the National Cyber Deception Laboratory - Cyber defence of our military networks needs to be militarised.

I am arguing that military cyber defence is currently and understandably dominated by passive civilian principles of security. For example, we put that which we value safely behind 'lock and key'. These approaches to security can only work when violations of that 'lock and key' cordon, are met with a response. When these cordons are broken in our society, that is when we turn to the state. It is the state, and the state alone, that backs up that right to security by its willingness to **fight** for it. Ultimately, it is the role of our armed forces to make that fight.

Our armed forces profoundly understand the use of aggression and violence within combat. Their unique burden is to wield the lethal capacity and have the moral courage to kill our enemies. They organise and succeed in this role through the willingness to sacrifice themselves and their colleagues. We entrust them to make unenviable decisions to defend our society and its values, decisions which will unavoidably inflict collateral damage. Fighting and striving to win is the fundamental purpose that defines their existence. **Their organisational culture and structures are wholly underpinned and orientated towards this mission, except perhaps in cyber defence.**

What current doctrine or policy enables today's digital warfighters to necessarily and aggressively defend our home territory in the way that the Auxiliary Units were tasked? Civilianised models of cyber defence reject the most fundamental features of combat; that people are going to get hurt; that those people include the defenders, and that there will be collateral damage from the fight. **Military networks need a full spectrum military defence.**

So if we think we should fight, how do we fight within this unprecedented operational environment? One perspective on this might be that we start by actively defending our home networks in the same way as the Auxiliary Units sought to defend our home soil. In our current context, this means attacking the digital, psychological and physical bodies of those that are assaulting us. The rules of engagement in military operations allow troops to defend themselves if they come under direct fire. This retaliation can often and necessarily precede investigatory attempts to identify who it is that is shooting at them. The range of responses we ask our military professionals to choose between in these complex settings extends from 'courageous restraint' through to a truly shocking range of lethal options. The physical and psychological costs of this capability and choices it brings are understood within a framework of values and standards that have roots in centuries of experience. Across those same centuries, one consistent feature of operational activity has survived all the same evolutions of warfare and the societies that wage them - **Deception**.

Deception is a strategy used by predators and prey, by attackers and defenders. It offers a competitive and evolutionary advantage that can be seen across the entirety of life on our planet, from the microbial organism through to the geopolitical stage of nation-states.

We are going to see today that deception offers us a vital opportunity within the unprecedented operational space of the cyber environment. Throughout history it has always provided the opportunity to level the playing field between the strong and the weak; the nearly defeated and their emboldened near victors.

Deception offers us a toolset to engage our cyber-enabled adversaries that our bombs and bullets cannot. It provides us with a way to fight when our digital rear area is overrun, whether you believe that to the case now or you accept it will happen in the future.

How do we bring deception into the digital fight?

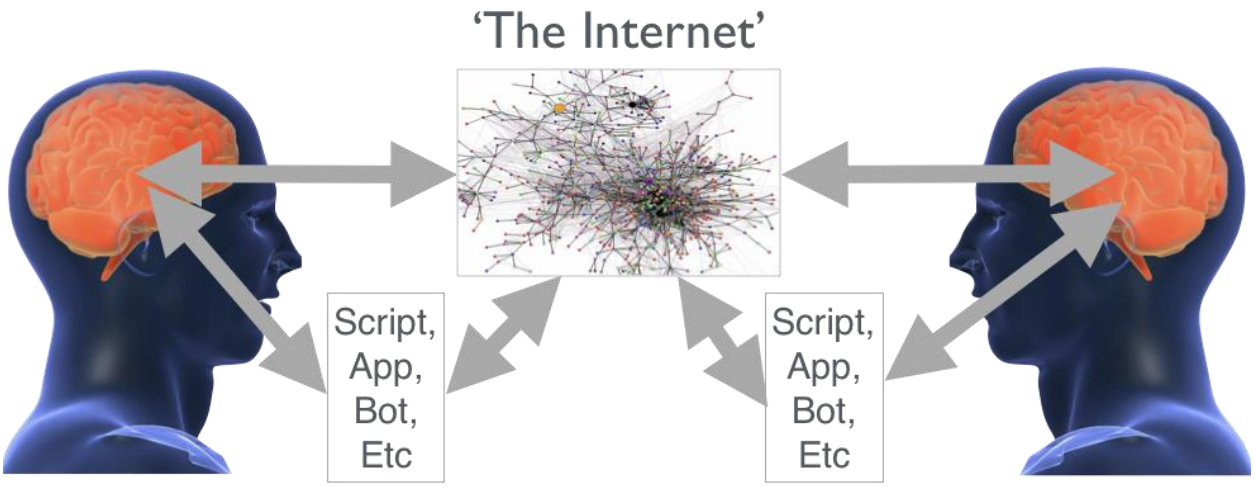
Here at the UK's Defence Academy, we run the Cyber Masters Postgraduate Programme. One of the first intellectually challenging activities of the course we ask of our students is to define cyber. Students here make many varied and meaningful responses to this task. This variety represents a series of credible and at times, competing views on the same topic. When trying to manage such complexity, we have to accept that different is not wrong. Applying this licence to explaining the concept of cyber in an adversarial context, we might see it as describing the sensemaking apparatus of our adversaries. As it can also be considered as the sensemaking

apparatus of our defences.

My colleague Simon Henderson explains sensemaking as the executive processing of information to generate action. Simply stated, it means: *"What's going on, what does this mean, and what should I do about it?"*

The outputs of sensemaking include: Meaning; Significance; Deductions; Inferences; Temporality; Beliefs; and Intent.

Deception is all about creating errors in the sensemaking of our adversaries. Its purpose is to get them to act in ways that suit our purposes, not theirs. Traditionally this cognitive attack surface is well understood by military commanders. However, today's operating environment extends to take in the synthetic elements of information systems and the networks they rely on. In this way, we can see the Cyber element of warfare as a proxy battle between combatants (slide)



Henderson, 2017

Because of the need to strike at both the sensemaking of the attackers and the sensemaking of the attack systems they deploy, we need to reframe cyber adversarial relationships. We need to move away from seeing cyber like a distant geospatial standoff of discrete reciprocal missile strikes; to cyber warfare as a constant multitude of intimate knife fights in a telephone box, with feints and disabling strikes through the deceptive telestimulation of our adversaries.

Cyber deception is going to be a central component of an inevitable arms race that has already started. This arms race will not be won through stockpiling capability and threatening its release. This is because there is or will be, no defensible rear area in which to store or hide it.

This means that cyber deception capability will need to be constantly developed and spent.

As a result, this leads us to an operational context where cyber deception will be expected! It perversely - won't be a surprise. This is a strength, not a weakness. The enemy's potential expectation of deception in warfighting goes as far back as that same history of warfighting. It is this expectation that can be manipulated to achieve proactive effects in the defence of our networks.

To those that seek to attack our future military networks, nothing will be what it seems. There will be no aspect of networked combat infrastructure, whether it's a deployed headquarters, a naval frigate or a fighter bomber, which will not carry deception assets and therefore the potential to displace, disrupt or even deliver a reciprocal strike back at the attacker.

The use of deception increases risk, but deception works!

Research into the use of deception in warfare consistently demonstrates this advantage.

"...although deceivers face many uncontrollable contingencies which threaten their plans, deceptions almost always result in advantages for those who attempt them."
Deception Research Group, Naval Postgraduate School, 1980

"It can accurately be stated that deception nearly always succeeds, at least to some degree. Indeed it should be emphasised that deception may succeed even when one or more causes for failure is present."
Maxim, D. (1982). Deception failures, non-failures and why. Washington: Office of Research and Development (Deception Research Program), Central Intelligence Agency.

With these observations in mind, here is **The National Cyber Deception Laboratory Mission Statement:**

To be recognised as the UK's nexus for cyber deception in proactive cyber defence

The NCDL is a project bigger than one institution. It will be a non-profit community of interest seeking to bring together those defending our networks with the suppliers and researchers that can support them in their mission. The lab community's role will be to challenge ourselves to think the previously unthinkable and discuss and debate the problems we potentially don't know we have yet. **Our remit is to support the militarisation of cyber defence through the use of deception as an inevitable step that must be considered, expanded and delivered upon.**

This purpose brings me to formally welcome you all to our inaugural event!

Today you will hear from the frontline thinkers and operators that form the vanguard of our future larger community. The breadth and complexity of the issues they will bring to your consideration are not presented as an easy set of answers. For each exciting potential opportunity that you spot, there will be a long tail of issues and problems for their implementation. This is a necessary challenge for any activity in this operational space. The UK military is a force for good, operating with transparency and legal accountability within a liberal western democracy. The use of cyber deception has to be adopted with rigorous intellectual professionalism. Then, and only then can the fight be taken out to those that seek to attack us. **Then, and only then can our currently benign enterprise networks become - like the gentle rural countryside and busy towns of Southern England in 1940 - a killing ground for our adversaries.**

Darren Lawrence
Director of the National Cyber Deception Laboratory
Course Director for the Cyberspace Operations MSc
Head of the Information Operations Group,
Senior Lecturer in Behavioural Science, Cranfield Defence and Security at the Defence Academy of the United Kingdom

Nov 2019