Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Ph. Lester and S. Moore, *Connections QJ* 19, no. 1 (2020): 39-44
https://doi.org/10.11610/Connections.19.1.04

Policy Article

Responding to the Cyber Threat: A UK Military Perspective

Air Commodore Phil Lester, Royal Air Force
and Captain Sean Moore, Royal Navy

Abstract: The article reviews the UK military contribution to the national approach to cybersecurity, extending across the continuum of inter-state activity from peace, through cooperation, competition, confrontation, conflict, and war. According to the UK doctrine, the military performs active and passive defensive functions in cyberspace, offensive cyber operations, cyber intelligence, surveillance and reconnaissance, and cyber operational preparation of the environment, and the response actions are not limited to just the cyber domain.

Keywords: military cyber capabilities, cyber operations, strategic defence review, fusion doctrine.

In 2015 through the UK *National Security Strategy and Strategic Defence Review*, the Government recognised the growing threat to our national stability, security and prosperity from activities occurring in, and from, cyberspace. Our national cyber capability supports our strategic objectives through three core functions: preventing conflict and threats materialising; protecting the UK and its overseas territories from attack particularly (but not exclusively) in, and through, cyberspace; and projecting influence and power rapidly and responsively, either directly from the UK or as part of an expeditionary operation.[1] These are national functions and the military has a contributory role in each, yet we recognise that any military contribution sub- and post-threshold, must be viewed as an extension of politics.[2] Thus, the military contribution is very much a supporting func-

[1] Ministry of Defence, "Cyber Primer," Second Edition (Shrivenham, UK: Development, Concepts and Doctrine Centre, July 2016), 2.

[2] Pre- or sub-threshold may be considered as an ability to deliver mass (and un-attributable) effect without triggering a meaningful response, thus blurring what has been

tion of a wider fused, pan-national response and applied in accordance with applicable law, including—where a state of armed conflict exists—International Humanitarian Law (aka Law of Armed Conflict or the Law of War). In this short article, we seek to outline the military contribution to a national approach and how existing international legal and normative frameworks provide a sufficient basis for operations in, from and through cyberspace.

While cyberspace is recognised as a warfighting domain in NATO and UK national military doctrine, it also has far-reaching non-military aspects that affect our daily life.[3] For these reasons, activities in cyberspace must be compliant with the rules-based international system. As such, we recognise that there are boundaries of acceptable state behaviour in cyberspace, just as there are everywhere else. In 2013, the UN Group of Governmental Experts on the use of cyber technologies affirmed the application of existing international law to states' cyber activities. On 26 June 2015, the UN Expert Group, including not just the UK and the US but also Russia and China recognised that the UN Charter applies in its entirety to cyberspace. The Group affirmed the relevance of a state's inherent right to act in self-defence in response to a cyber operation meeting the threshold of an armed attack. In addition, the 2015 Report confirmed that the fundamental protections of international humanitarian law—necessity, proportionality, humanity, and distinction—apply in cyberspace.

A version of this article has been presented to a recent Cyber Norms conference held at MIT, Boston. Much of what we say has resonance with this publication and we have therefore used our previous work as a foundation for inclusion in this journal.

Accordingly, Defence's cyberspace activities, whether enabling military action or supporting wider government activities, extend across the continuum of inter-state activity from peace, through cooperation, competition, confrontation, conflict, and War. The reality of increased hostile state activity through cyberspace and below the threshold of armed conflict infers increasing concern of the growing risk of increasingly destructive cyberattacks, as well as potentially the non-intended collateral damage effects of an attack elsewhere on our own infrastructure. This reality requires us to look at how the military instrument might be employed to counter such threats and activities in a period of persistent competition and below the threshold of armed conflict.[4] To address this requirement, we should unpack some of the themes that might be derived from the title, such as 'response', 'fusion', 'discretion': the 'should' or 'could' and place them into the wider context including framing a five domain—that is an inte-

normal, and hence tolerable, state competition. This is not simply a narrow band which sits on the boundary of peace and war but a fluid and variable space which can be manipulated across time, domains and environments.

[3] Joint Doctrine Publication 0-01 UK Defence Doctrine, 6th Edition (Draft).

[4] "Persistent competition" might be defined as intense hostile state activity outside the rules-based international system and below the threshold that might result in armed conflict.

grated air, space, cyber, maritime, and land—military contribution through our Joint Action operating model to achieve the military objective of a national strategy.[5]

First, the use of the word 'response' has significant negative connotations – it is reactive and implies a degree of passivity before action. All too frequently, we see response used in conjunction with military – "the military response." But this hides the inherently offensive nature, and the utility of pre-emptive qualities, of the military instrument. It must be recognised that hard kinetic action is not always appropriate or indeed necessary. The military has more to offer than just binary offensive or defensive capabilities. So, the point to emphasise here is that there is a broad range of military options that have wide utility for application, contributing to a fused national approach left of an adversary's strike or in the zone of sub-threshold persistent competition. This could be to either contribute to an anticipatory deterrence or coercion strategy as well as to contribute to our overall national security approach. Yet, we should recognise that the military contribution may not, of course, be a cyber one. So, our ability to contribute more effectively "left of bang" as we like to say, requires resource and political appetite to do so. It must be exercised and tested to prove the approach – and this should not be solely a military enterprise. It needs to be 'fused' with others – the Intelligence agencies, government, other government departments, industry, and the critical national infrastructure as examples. We talk of persistent competition from our adversaries; therefore, our approach must be one of persistent engagement—physical, virtual and cognitive—utilising all levers of national power, diplomatic, information, economic, and military to demonstrate national resolve and determination but also to ensure we retain a competitive advantage.

This leads on to 'fusion' and, by implication, the UK Government's Fusion Doctrine. The principles behind Fusion Doctrine, we contend, are nothing new. We have had an "integrated approach," "comprehensive approach," and the "full-spectrum approach" – all designed to fuse cross Whitehall activity. Yet, the Fusion Doctrine goes further as it inculcates a real sense of joined-up thinking and practice to deliver successful outcomes against multiple challenges. A strategy to deter adversaries is a key function of the Fusion Doctrine. And the deterrence of cyber aggression or cyberattacks needs to include all aspects of our national life with all sectors ensuring that they should consider their response, not in isolation, but coherent, consistent, and coordinated with others. As a result, our approach to modern deterrence is somewhat different from the deterrence

[5] "Joint action" is our framework approach to integrate information activities with fires (lethal and non-lethal effects), manoeuvre and outreach to gain competitive advantage – placing influence as a primary outcome, and integration at its core as the principal enabling tenet. Tempo and the precision of effect will continue to be generated, predominantly (but not solely), by a joint force, planning and executing operations within and across multiple domains rapidly, to maintain the initiative and pose the adversary with multiple insoluble dilemmas.

of the Cold War. Deterrence today needs to be a more nuanced use of hard and soft power with all departments contributing to fused strategies to deliver specific deterrence strategies for specific threats and behaviours.

So, what 'could' the military do? This needs to be broken down into two parts: the generic contribution, what we do, and care for, in support of Government priorities as well as the specific cyber role. Turning first to our generic contribution.

Through the military, the Government exercises its right to the legitimate use of force and such force is used to further political objectives, primarily the security of our nation. Our objectives are clearly defined in the National Security Strategy and within defence policies. From these objectives, a range of military tasks is defined and resourced.

Possession of capable, professional, and well-trained militaries also gives governments a broader set of response options to cyber threats. As the former UK Attorney General said, "States that are targeted by hostile cyber operations have the right to respond to those operations in accordance with the options lawfully available to them…"[6] A hostile cyber operation does not necessitate a cyber response. All lawful options, including an armed response when appropriate, are open to states that are attacked.

While the UK's armed forces are primarily resourced and configured to defend our national security, our broad maritime, land, air, space and cyber capabilities can be made available to support other crises, such as humanitarian aid and military aid to government departments. Thus, our response to a crisis or event brought on by actions in cyberspace could include the full range of conventional military capabilities to the use of limited or discrete functions and roles. This is not dissimilar to that seen during the foot and mouth outbreak in the UK in 2001, the fire service strikes or during flooding where military capability has been used to reinforce governmental departments or civilian organisations. But one area where the military could provide a very worthwhile generic support function is through our command and control organisations which are designed around the delivery of an integrated, cross-function liaison, coordination, and control output. These headquarters are adept at fusing multi-source intelligence and information to direct activities and would also be able to communicate the defence contribution and ensure that it is dovetailed into wider narratives. Our headquarters are also good at applying the rules of engagement and standards of proportionality and discrimination on the use of military capability – whether it be a non-lethal or lethal force. Thus, we believe that the military is good at self-restraint and uses tested processes to increase and decrease the use or the threat of force to achieve the desired outcome. We also utilise "plugs and sockets" to introduce non-organic or non-defence structures into our decision-making architecture. Combined, this allows effective, rapid, and evidence-based decision-making processes.

[6] Speech by Jeremy Wright QC to Chatham House on 23 May 2018.

Let us turn to the specific cyber contribution. Our UK doctrine clearly spells out how defence breaks down its operations in cyberspace and how these contribute to delivering military effect and supporting wider political objectives. We will not go into the detail here—much of it remains classified—but it is safe to say that our doctrine outlines the following cyberspace functions: defensive[7] (active[8] and passive[9]) as well as offensive[10] cyber operations, cyber intelligence, surveillance and reconnaissance[11] and cyber operational preparation of the environment.[12]

From the perspective of what the military *'should'* contribute, our approach is twofold. First, we must continue to mainstream our cyberspace thinking and actions across our whole force. Doctrine and education are key here. Because of the sensitive nature of the cyber domain, our doctrine is currently classified, and this has limited its accessibility and hampered our ability to increase understanding of cyber operations across the UK military. We are now exploring ways to increase the accessibility of our cyber doctrine to enhance its application as part of our approach to developing five domain integration (maritime, land, air, space as well as cyber). In parallel, we are embarking on a journey to develop some cutting-edge conceptual thinking to guide future iterations of our doctrine, education, and practice. Combined, these will increase our cyberspace awareness, our agility, and, therefore, our utility by generating warfighters capable of operating in cyberspace rather than producing cyberwarriors – although we do need some of the latter! The second element must continue to bring focus on what we need to do to ensure our networks and interfaces are as resilient as possible and that our defensive measures are consistent and coordinated with those who legitimately have access to or share our systems. This is not an easy challenge, especially the need to ensure cyber resilience in all our developmental programmes as well as ensuring that our legacy programmes and capabilities can adapt to the rapidly changing threat dynamics in cyberspace now and into the future.

So, to conclude, the military can provide a significant contribution to the cyber threat and much of that is already in train. We must also recognise that undoubtedly the largest contributions we can make are threefold. First, ensuring our own cyber defence is robust and resilient, including guaranteeing that it is consistent and coordinated with the defensive approaches of others who share our networks. Second, our response or contribution may not be in the cyber do-

[7] Active and passive measures to preserve the ability to use cyberspace.

[8] Activities that target hostile offensive cyber operations to preserve our freedom of manoeuvre within cyberspace.

[9] Threat specific defensive measures to reduce the effectiveness of cyber activity.

[10] Activities that project power to achieve military objectives in, or through, cyberspace.

[11] Intelligence, Surveillance and Reconnaissance (ISR) activities in, and through, friendly, neutral and adversary cyberspace to build understanding.

[12] All activities conducted to prepare and enable cyber ISR as well as defensive and offensive operations.

main itself. Third, our command and control structures provide a very useful reference point from which we could develop a fused strategic headquarters that coordinates and directs our national cyberspace operations. These can only be realised if Defence continues to invest in mainstreaming cyberspace as both a threat and opportunity in our strategies, doctrine, and practice. Yet returning to the question, effective fusion can only be achieved through practice, exercising, and testing … until it becomes second nature.

Disclaimer

The views and opinions expressed are solely those of the contributing authors and should not be taken to represent those of Her Majesty's Government, Ministry of Defence, Her Majesty's Armed Forces or any UK government agency, the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgement

Journal *Connections: The Quarterly Journal*, Vol. 19, 2020 is supported by the United States government.