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

Oliver Fitton, *Connections QJ* 15, no. 2 (2016): 109-119
http://dx.doi.org/10.11610/Connections.15.2.08

Research Article

Cyber Operations and Gray Zones: Challenges for NATO

Oliver Fitton

Politics, Philosophy & Religion Department, Lancaster University,
http://www.lancaster.ac.uk/

Abstract: The Gray Zone represents a space between peaceful state rivalries and war. Within this space actors have developed hybrid strategies to extend their influence. This concept of conflict is best illustrated by Russia's actions in Eastern Ukraine in 2014. Gray Zone doctrine leverages ambiguity to create an environment in which adversaries are unable to make strategic decisions in a timely and confident manner. Cyber Operations, because of the attribution problem, lend themselves to this kind of conflict. This article explores the interactions between the Gray Zone and cyber operations and considers questions which NATO must address in order to adapt.

Keywords: cyber war, gray zone, ambiguity, NATO, hybrid war.

Introduction

Russia's annexation of Crimea in 2014 represented a severe challenge to NATO. The events that took place in Eastern Ukraine involved a hybrid strategy, which relied heavily on ambiguity. Strategists in Moscow used conventional forces, a grip on Russian-language media, a loose interpretation of international law, local proxies, information operations and cyber operations as tools to operate within the gray zone between war and peace. Although what Russia achieved in Crimea represented more than peaceful competition between states, it was achieved without triggering a large-scale military engagement.

In 2007 Russia launched another gray zone operation that navigated the fine line between war and peace. The denial of service attack that crippled Estonia in April of that year was the result of tensions between the two countries boiling over. Russia did not employ an armed response, which would inevitably invoke Article 5 of the North Atlantic Treaty. Instead, a new kind of deniable operation was used, which lent itself to the gray zone: a cyber operation.

It is argued throughout this article that cyber operations have and will continue to be an effective tool for the adversaries of NATO as part of a gray zone strategy. The nascent concept of the gray zone will be explored and its relationship with hybrid warfare elucidated. The applicability of cyber operations to gray zone strategy will be discussed in terms of the problem of attribution for the victim and the advantage deniability affords for the attacker. Finally, three challenges NATO faces as a result of cyber operations within the gray zone will be presented. Firstly, the challenge ambiguity represents to Article 5 of the North Atlantic Treaty; secondly, achieving deterrence against limited operations that erode NATO influence; and finally, how to navigate this new norm of conflict that liberal democratic principles prohibit. It is beyond the remit of this article to solve these problems; the objective is rather to compel the academic community to engage with the challenges of the gray zone and how cyber operations will be assimilated into future strategies.

The Gray Zone

The gray zone between war and peace is the primary characteristic of modern conflicts. Carl von Clausewitz considers war to be an extension of a duel between two parties, "an act of violence intended to compel our opponent to fulfil our will." [1] For the majority of human history this definition of war was self-evident. From the Peloponnesian War onwards a state of war involved a known adversary with clear political objectives in opposition to one's own. According to General Curtis LeMay, winning wars was simple: "You've got to kill people and when you kill enough of them, they stop fighting." [2] Clausewitz's definition of war imbues with unchanging characteristics – war is violent, instrumental and political.[3] However, recent attention in academia and policymaking (especially within NATO) to concepts including hybrid wars, ambiguous wars and limited wars suggests that the character of war is changing – or at least the threats the Alliance faces are becoming less easily defined.

Of the scholars from multiple disciplines who have engaged with the concept of hybrid warfare over the years,[4] Frank Hoffman is perhaps the most widely quoted. According to his definition, hybrid warfare is a deviation from

[1] Carl von Clausewitz, *On War*, ed. Anatol Rapoport (Harmondsworth: Penguin Books, 1982), 101.

[2] Richard Rhodes, *The Making of the Atomic Bomb* (London: Simon & Schuster, 2012), 586.

[3] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

[4] See e.g. Larry R. Jordan, *Hybrid War: Is the US Army Ready for the Face of 21st Century Warfare*, Master's thesis (US Army Command and General Staff College, 2008); Mackubin Thomas Owens, "Reflection on Future War," *Naval War College Review* 61:3 (2008): 61–76; and Russell W. Glenn, *All Glory Is Fleeting: Insights from the Second Lebanon War* (Santa Monica, CA: RAND, 2012).

previous incarnations: “Instead of separate challenges with fundamentally different approaches (conventional, irregular, terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously.”[5] The paragon of such doctrine for Hoffman was Hezbollah in the 2006 Second Lebanon War, during which Hezbollah repelled a vastly superior Israeli conventional force through the use of both conventional and unconventional tactics.[6] Following Hoffman’s interpretation of hybrid threats, the United States (US) will more frequently contend with adversaries capable of employing conventional weapons such as anti-tank and cruise missiles and unmanned aerial vehicles, while using irregular tactics such as hiding among the civilian population and improvised explosive devices. There is limited literature on cyber operations and their significance within hybrid strategies.[7] However, there is a much greater discussion surrounding the concept of cyber war as a distinct concept that is highly pertinent to the subject of hybrid war and gray zone conflict.[8]

Gray zone conflict and hybrid war are not interchangeable concepts. Indeed, the use of the term “conflict” for the former and “war” for the latter is deliberate. The use of “unconventional” and “irregular” tactics is not limited to the strict Clausewitzian paradigm of war. The concept of the gray zone seeks to encompass operations that fall short of warfare due to intensity, legality or (most interestingly) ambiguity. Unconventional tactics can involve information, psychological, diplomatic or economic operations outside the definition of “warfare” if it is to be used in any meaningful sense. NATO commanders have begun to publically express concern over such unconventional threats.[9] It is the extensive use of unconventional tactics outside of strictly defined wartime that has contributed to a crisis in confidence within NATO.[10] US Special Operations Command is embarking upon a yearlong research project entitled *The Gray Zone*. The project aims to give the US government the tools to understand gray zone threats and create effective responses to them. The gray zone is defined

[5] Frank G. Hoffman, “Hybrid Warfare and Challenges,” *Joint Force Quarterly* 52 (2009): 35.

[6] Ibid., 37.

[7] See Sascha-Dominik Bachmann and Hakan Gunneriussan, “Hybrid Wars: The 21st Century’s New Threats To Global Peace And Security,” *Scientia Militaria, South African Journal of Military Studies* 43:1 (2015): 77–98.

[8] See e.g. John Arquilla and David Ronfeldt, “Cyberwar is Coming!” *Comparative Strategy* 12:2 (1993): 141–165; Richard A. Clarke, *Cyber War: The Next Threat to National Security And What To Do About It* (New York: HarperCollins, 2010); and Rid, *Cyber War Will Not Take Place*.

[9] John Vandiver, “Breedlove: NATO Must Redefine Responses to Unconventional Threats,” *Stars and Stripes*, 31 July 2014, http://www.stripes.com/news/breedlove-nato-must-redefine-responses-to-unconventional-threats-1.296129 (accessed 23 January 2016).

[10] Peter Apps, “‘Ambiguous Warfare’ Providing NATO with New Challenges,” *Reuters*, 21 August 2014, available at http://uk.reuters.com/article/uk-nato-summit-idUKKBN0GL1KA20140821 (accessed 23 January 2016).

as the region between peace and war, which is not yet fully understood. Actions undertaken in the gray zone go beyond normal peacetime competition but fall short of all-out war.[11]

Russian operations in Eastern Ukraine and Crimea had both a hybrid and ambiguous character. In 2014 Russia used a combination of conventional military forces (for example, amassing on the Russia/Ukraine boarder and naval patrols) and unconventional tactics (for example, "the little green men" and information dominance attained by leveraging Russian nationalism in East Ukraine) to secure the annexation of Crimea. These actions caused alarm throughout the Alliance despite Ukraine's status as a NATO non-member. Engineered uncertainty in Russian action and rhetoric crippled the Alliance's ability to respond and has the potential to do so again should the doctrine be employed against NATO members in Eastern Europe.[12] Whether these tactics were new or anchored with historical precedent remains a matter of debate.[13] What is clear, however, is that NATO is unprepared for gray zone conflict.

As demonstrated in Eastern Ukraine, ambiguity is a useful tool. Without a full picture of validated information, it becomes difficult for a strategist to choose the optimal course of action. By allowing ambiguity to feature within strategic decisions or by actively inserting ambiguity into strategy, it is possible to cloud the vision of enemy. The United Kingdom (UK) employs a policy of deliberate ambiguity in its strategic nuclear deterrent. As a result, adversaries of the UK are unaware of "when, how and at what scale"[14] the UK government would be willing to use nuclear weapons, including whether they would be used on a first-strike basis. A clear statement on the planned use of the nuclear deterrent would allow adversaries to more clearly calculate their own strategies. Ambiguity within strategic nuclear deterrence allows states to operate below the threshold of conflict by not explicitly threatening an individual adversary. It was a balance between known variables and ambiguous strategies that maintained stability during the Cold War.

[11] United States Special Operations Command, "The Gray Zone," White paper, 9 September 2015), 1, http://army.com/sites/army.com/files/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf (accessed 23 January 2016).

[12] For further discussion on this topic see House of Commons Defence Committee, *Towards the next Defence and Security Review: Part Two – NATO* (London: House of Commons Defence Committee, 2014), and in particular the evidence given to the Committee by Sir Bob Russell.

[13] Peter R. Mansoor discusses this debate, which centers on competing definitions of "hybrid warfare," in "Hybrid Warfare in History," introductory chapter in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012).

[14] HM Government, *The Future of the United Kingdom's Nuclear Deterrent*, December 2006, Cm 6994, at 18.

Gray zone strategy is employed by non-liberal democratic states and authoritarian non-state actors. Such strategy, especially the use of ambiguity, is antithetic to societies based upon social pluralism, binding legal principles and government accountability. Accountability and transparency are especially sought after in public discourse regarding military action following the invasion of Iraq in 2003 and the publication of the infamous "dodgy dossier."[15] Such desire was palpable in the UK during the recent debates over intervention in Syria. Democratic accountability functions to limit the degree to which governments can employ ambiguity.

Russia, however, is unrestrained by social pluralism and government accountability. Dissent has been met with violence.[16] Putin's administration has a strong grip over the majority of the Russian speaking media in the region.[17] Russian decision making is dramatically less transparent than that of NATO members. Russia is therefore relatively unrestrained in its ability to employ both conventional and unconventional operations against their adversaries. Daesh represents freedom of operation to an even greater degree, owing to its disregard for international law. In a straightforward Clausewitzian scenario, war is clearly understood and established rules of engagement apply. NATO is designed to win these wars. In gray zone conflict it is not clear who the enemy is or what their intentions are, forcing liberal democracies to question the legitimacy of their responses with much greater scrutiny than non-democratic actors. Liberal democracies are greatly restrained in situations where autocratic states and non-state actors are not. This results in a strategic imbalance that threatens and undermines the strategic advantage NATO provides.

Cyber Operations

As NATO's adversaries develop strategies to exploit the gray zone, conventional force is likely to be used in new ways and new unconventional tactics will appear. Some unconventional tactics are likely to be more effective than others. Cyber operations represent a developing unconventional approach that can be highly effective within gray zone conflict.

Cyber operations are facilitated by reliance on networked communication. They exclusively utilize computer code in order to alter, collect data from or deactivate computer systems that have software, hardware and human components. Cyber operations cannot be directly violent because computer code

[15] The poorly researched and attributed intelligence report that claimed that Iraqi weapons of mass destruction could be readied for use within 45 minutes. This dossier was employed by the Blair government to support the argument for military intervention in Iraq in 2003.

[16] For example, the death of Boris Nemtsov in February 2015 and the violent suppression of members of the music group Pussy Riot during their demonstrations at the 2014 Sochi Winter Olympics.

[17] Scott Gehlbach, "Reflections on Putin and the Media," *Post-Soviet Affairs* 26:1 (2013): 78.

cannot directly damage a human in the same way as kinetic, energy or agent-based weapons.[18] Nevertheless, they have become a notable element of modern conflict, including being used to shut down nuclear enrichment facilities[19] and spy on governments.[20] In the recent UK National Security Strategy and Strategic Defence and Security Review 2015, the government committed £1.9 billion to "protecting the UK from cyber attack and developing … sovereign capacities in cyber space."[21] Cyber operations are of particular value in gray zone conflict thanks to two key characteristics: inherent problems associated with attribution and deniability on the part of the attacker.

For adversaries who want to make strategic gains without reaching the conflict threshold laid down by NATO (Article 5), the idiom "on the Internet no one knows you're a dog" rings particularly true. Anonymity is a central characteristic of activity in cyberspace. Attributing cyber attacks to adversaries (be they individuals, non-state actors or nation states) is complex, time consuming and challenging. Furthermore, it is unlikely that the resulting verdict of attribution will be so certain as to justify a traditional military response. Therefore, the deterrence effect that NATO has been so successful in achieving in terms of armed conflict in Europe does not apply to cyber operations. Indeed, many NATO members have been struck by various forms of cyber attack, most notably the large-scale denial of service attack against Estonia in 2007.[22]

In 2015 Thomas Rid and Ben Buchanan assessed the attribution problem in an attempt to understand its challenges and advise policymakers on a potential solution. They concluded that attribution analysis is an art form requiring "skill, tools as well as organizational culture: well-run teams, capable individuals, hard-earned experiences and often and initial, hard-to-articulate feeling that 'something is wrong.'"[23] Further, they warn that attribution is not a binary matter of possible versus impossible. Rather, attribution can be achieved with varying levels of certainty. Perhaps most importantly, Rid and Buchanan point out that attribution is a matter of political will: it depends on the resources that governments want to put into tackling it.

Rid and Buchanan developed a system they call the "Q Model" for attribution. This model requires three layers of scrutiny including tactical (technical),

[18] Rid, *Cyber War Will Not Take Place*, 13.

[19] For further details on the Stuxnet incident see Nicolas Falliere, Liam O. Murchu and Eric Chien, *W32.Stuxnet Dossier* (Cupertino, CA: Symantec Corporation, 2011).

[20] For further details on the GhostNet incident see "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, 29 March 2009.

[21] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015, Cm 9161, at 40.

[22] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," White paper presented at the 2008 Black Hat Conference, 7.0.

[23] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2015): 30.

operational and strategic analysis. At the tactical level, technicians identify that an attack has taken place and use all the tools at their disposable to understand the *how* of the attack. How did the adversary gain entry to the system and how did they create an effect after successful access? This stage of analysis may focus on tracking Internet Protocol (IP) addresses, observing the adversary's movement around the system in question, reverse engineering of malicious code and a host of other technical skills. At the operational level, the technical analysis is compiled and assessed alongside other sources of information, such as non-technical analysis (possibly signals intelligence and human intelligence), analysis of similar attacks and the wider geopolitical context to create hypotheses about what happened – the *what* of the attack. Finally, the strategic layer attempts to understand the *who* and the *why* of the attack. At this point, decision-makers consider the operational hypotheses, debate who may be responsible and formulate a response based on the attack's significance. The final aspect of the Q Model is to communicate attribution to the wider community.

However, this model does not solve the problem of attribution. Advanced adversaries will still be able to obfuscate their role in cyber operations to a certain degree, most likely by pointing the finger at another actor. This can be achieved with the use of a certain language or skillful placement of what appear to be coding mistakes. Rid and Buchanan point out that "The perfect cyber attack is as elusive as the perfect crime."[24] However, adversaries in hybrid war do not need to achieve the perfect unattributable cyber attack; they simply need to cause enough doubt in the minds of analysts to limit or slow policy-maker's responses.

The second characteristic of cyber operations that is particularly important to understand in the context of hybrid strategies is deniability. There is an increasing trend towards deniable partnerships between states and cyber operations specialist groups, which insulates the state from blame for disruptive unconventional campaigns. During the early stages of the civil war in Syria, President Bashir Al-Assad's regime developed an ambiguous relationship with a group called the Syrian Electronic Army (SEA). The SEA was a pro-Assad movement that hacked into Western websites and social media accounts, defacing them and spreading pro-Assad messages. High-profile targets included the *Onion*, the Associated Press (AP) and Harvard University.[25] However, the SEA was not Assad's personal cyber army, and their relationship was often publically strained.[26] As a result, Assad could plausibly deny that his regime was responsi-

[24] Ibid., 32.

[25] For further discussion of the activities of the Syrian Electronic Army and its attacks see Oliver Fitton and Mark Lacy, "The Syrian Electronic Army Is Rewriting the Rules of War," *The Conversation*, 3 September 2013, http://theconversation.com/the-syrian-electronic-army-is-rewriting-the-rules-of-war-17618 (23 January 2016).

[26] Adam Jones, "Syrian Electronic Army Turns on Assad Regime," *Seczine: Security Magazine*, 21 August 2013, http://seczine.com/cyber-security/2013/08/syrian-electronic-army-turns-on-assad-regime/ (accessed 23 January 2016).

ble for defacing Western websites and stealing data from US institutions while benefiting from the tactical success of the SEA. It has been suggested that Russia used the very same model to carry out cyber attacks on the Georgian government in 2008 and Estonian financial institutions in 2007 through the organization known as the Russian Business Network (RBN).[27]

Cyber operations are difficult to attribute and in some cases deniable even if a degree of attribution is possible. They also have the potential to be extremely dangerous. While computer code will never kill a human being directly, it is highly likely that cyber attacks on industrial or societal infrastructure will one day result in death. For example, in 2006 the Aurora experiment demonstrated that code-based exploits can result in kinetic effects,[28] and in 2010 the Stuxnet worm proved to be behind the malfunctions of centrifuges at the Natanz nuclear facility in Iran. The potential for both ambiguity and effectiveness means that cyber operations are very likely to be employed by gray zone adversaries in the future as they have been in the recent past.

Challenges for NATO

NATO recognizes that hybrid warfare is a strategy it must come to understand and learn to combat. NATO must take special notice of the role that cyber operations play within hybrid strategies with special emphasis on their ambiguous nature. Three specific challenges are apparent. First, there is the question of how to apply Article 5 of the North Atlantic Treaty in the case of a cyber attack on a NATO member state if attribution is not a binary proposition. Second, if attribution and deniability restrain NATO's use of force, the Alliance must find a way to deter adversaries from the use of low-intensity tactics, such as those employed in Estonia, Georgia and Eastern Ukraine. Finally, it remains to be seen whether NATO can employ cyber operations as part of a gray zone strategy while respecting the liberal democratic principles that separate the Alliance from its adversaries. In other words, it would be wise for NATO to engage in gray zone strategies.

Article 5 of the North Atlantic Treaty states that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." As such, the Alliance will take "action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[29] The first problem with Article 5 regarding cyber attacks is the debate around the degree to which cyber attacks represent an "armed

[27] Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet* (New York: Public Affairs, 2010), 212–213.

[28] Fortinet, "Securing SCADA Infrastructure," White paper (Sunnyvale, CA: Fortinet, 2010), 6.

[29] "The Atlantic Charter," last modified 1 October 2009, available at www.nato.int/cps/bu/natohq/official_texts_16912.htm.

attack."[30] If cyber attacks cannot be considered violent[31] there must be debate over their status as "armed attacks". If a cyber attack is not considered to be an armed attack, such an event does not automatically trigger the process of collective response on which European security has been based since the end of the Second World War. However, this view has been challenged in the wake of the 2007 cyber attacks against Estonia. NATO Secretary-General Jens Stoltenberg confirmed that NATO deems cyber attacks within the spirit of the requirements for action based upon Article 5 commitments.[32] This echoes the unilateral stance taken by the United States.[33]

The next question associated with this first challenge is how to justify a military response to a cyber attack invoking Article 5 when the process of attribution (as described by Rid and Buchanan) requires time, investment and a multilayered approach in order to produce a conclusion that is unlikely to be one hundred percent certain. Even if the legality of an armed response to a cyber attack is agreed upon, the confidence of NATO commanders in their actions must be based on the fallible science of attribution. Moreover, it will be difficult for NATO to react decisively if the adversary suspected of carrying out a cyber attack has a degree of built-in deniability, such as those between Russia and the RBN or Assad's regime in Syria and the SEA. Were cyber operations to take place alongside clear conventional military operations (as seen in Georgia in 2008), actions based on Article 5 would be clearly justified. If cyber operations were to precede the use of conventional tactics within a hybrid strategy, NATO may find itself constrained, divided and unable to act decisively as a result of an adversary engineering uncertainty through plausible deniability.

The second challenge NATO must overcome is how to deter cyber operations against NATO members. The full extent of a nation state's cyber capability is necessarily a matter of ambiguity. Should specific capabilities be revealed, the exploits upon which they are based are liable to be fixed and that capability rendered useless. This is a fundamentally different challenge compared to conventional and nuclear deterrence. While cyber operations may never be comparable to conventional or nuclear warfare to the extent that they represent an existential threat to a nation-state, it is likely that they may be used to destabilize societies, economies and populations within the sphere of influence of an adversary as part of a wider hybrid doctrine. Such destabilization may contrib-

[30] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 3.

[31] See Rid, *Cyber War Will Not Take Place.*

[32] Paul McLeary, "NATO Chief: Cyber Can Trigger Article 5," *Defense News*, 25 March 2015, available at www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930 (accessed 23 January 2016).

[33] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, 31 May 2011, available at http://www.wsj.com/articles/SB10001424052702304563104576355623135782718 (accessed 23 January 2016).

ute to the erosion of NATO's influence and ability to secure its strategic objectives.

The final challenge relates to how NATO's liberal democratic principles restrain it from employing the same tactics used by its adversaries, despite the opportunity to do so, and to achieve strategic success. NATO members, in particular the US and UK, have some of the largest investments in cyber operations. However, they are the nations that will be the most constrained from using such unconventional tactics openly. Liberal democratic principles including the rule of law, government accountability and transparency should restrict these states from employing their unconventional operations during peacetime. As a result, NATO is at risk of being left in a doctrinal deficit more difficult to overcome than any technology gap. NATO's adversaries are thus able to take advantage of the gray zone between war and peace: Daesh can gain territory while spreading fear and its radical message and Russia is able to make territorial and psychological gains in Eastern Europe, while NATO itself is philosophically bound to uphold strict virtues. As a result, NATO stands to have its influence eroded while being unable to play the very game it is losing.

Nevertheless, pragmatism may inevitably come before virtue. Russia has long accused the West of using the very ambiguous strategies that Western academia now recognizes Russia to be employing.[34] According to Timothy L Thomas, Russian scholars have long viewed the Soviet defeat to be the result of a clandestine information war.[35] There are question marks around how sustainable such a doctrine might be in the modern age. It is entirely possible that NATO members could create deniable relationships with online non-state actors in order to achieve the kinds of deniable partnerships that have been enjoyed by Assad and Putin. Indeed, this may be easier for liberal democratic states. The principles of many online groups often include liberty, equality and positivism, if not rule of law. However, any evidence of such partnership is likely to cause some tension between populations and governments in a post Wiki-leaks world. Furthermore, the deniability enjoyed by adversaries comes at the cost of command and control, which can lead to unintended consequences for highly networked societies. As a result, deniable partnerships are unlikely to be appealing in a NATO gray zone strategy.

Conclusion

Gray zone conflict marks an extension of hybrid warfare into the space between war and peace. It employs both conventional and unconventional methods to achieve political goals, as well as ambiguity to cloud the judgement of adversaries. Cyber operations are an unconventional tactic that has been and

[34] Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles: Potomac Books, 2009), 486.

[35] Ibid., 477.

will continue to be used in gray zone approaches by NATO’s adversaries. Issues surrounding the attribution of cyber operations and engineered deniability on the part of adversaries drastically restrain NATO’s ability to respond to cyber operations. It is vital that NATO develop a means by which to respond and deter such tactics, not only because of the damage cyber attacks might cause, but also because of their potential to erode NATO’s influence in contested spheres.

About the author

Oliver Fitton is a PhD candidate in the Department of Politics, Philosophy and Religion at Lancaster University, UK and a researcher for Security Lancaster, a GCHQ Centre of Excellence in Cyber Security. His research focuses on cyber operations and ambiguity in modern and future conflict.
E-mail: o.fitton@lancaster.ac.uk.