Wilton Park

Image: posteriori

Report

Military operations in cyberspace

Wednesday 5 – Friday 7 September 2018 | WP1635

In association with:

GO ROOT
ACCESS INTELLIGENCE

Australian Government
Department of Foreign Affairs and Trade

With reception sponsored:

Microsoft

EXEDEC

Wilton Park

Report

Military operations in cyberspace

Wednesday 5 – Friday 7 September 2018 | WP1635

In association with NATO Defense College, GoRoot Ltd, The Australian Department of Foreign Affairs and Trade and Microsoft Corporation.

Following an opening session in which two speakers (one non-military, one military) addressed the question 'Is cyberspace a battlespace?', the conference worked through the various phases of a hypothetical military operation in cyberspace: the prevention of conflict (including deterrence); the means available for conflict in cyberspace (eg cyber weapons, dual-use platforms); the justification for military operations (eg threats, offence-defence balance); the conduct of operations (in two parts – operational and strategic); the mediation of conflict (eg conflict management, de-escalation); legal and ethical constraints on military operations in cyberspace; the conclusion of military operations (including the notions of victory, defeat and loss); and finally, a discussion of plausible futures for military operations in cyberspace.

Speakers were invited to speak for no more than 10 minutes to allow significant time for roundtable discussion. The participatory format of the meeting helped generate fresh insights and analysis. It was held on the basis of non-attributable discussion in a neutral environment designed to encourage an open and constructive exchange. Meeting outcomes are captured in this report summarising the discussions, conclusions, policy recommendations, and actions, which will be widely circulated to interested parties and posted on Wilton Park and other websites.

Summary

The human race has a propensity for conflict; on land, at sea, in the air and to some extent in outer space. Has cyberspace become the latest 'battlespace'; a recognisable domain of military activity in which the organised armed forces of states should have specific roles and responsibilities? 'Military operations in cyberspace', a conference held at Wilton Park in early September 2018, set out to answer these questions from a variety of perspectives – operational, political, legal, moral, strategic and technical.

Rather than follow a standard, thematic agenda, Military operations was structured sequentially. The conference began by asking why and how cyberspace might indeed be understood as a battlespace. Discussion then addressed in turn the more or less discrete phases of a notional conflict in cyberspace: the **prevention** of conflict (including deterrence); the **means** available for conflict in cyberspace (e.g. cyber weapons and dual-use platforms); the **justification** for military operations (e.g. threats, the balance between offensive and defensive capabilities); the **conduct** of operations (in two parts – the tactical/operational and the higher level strategic); the **management** of conflict (e.g. conflict mediation and de-escalation); legal and ethical **constraints** on military operations in cyberspace; and the **conclusion** of military operations (including the notions of victory, defeat and loss). The conference finished with a discussion of plausible **futures** for military operations in cyberspace.

The conference highlighted above all that the national security communities and militaries of technologically advanced democracies are struggling to understand the character and

implications of all of these phases of potential conflict in cyberspace. The concluding section of this report is almost entirely devoted to raising a series of intricate and urgent questions that need further reflection. One certainty though is that militaries cannot effectively undertake this reflection on their own and that it must be conducted as part of a comprehensive, integrated civil-military approach to conflict in cyberspace.

Introduction

1. If war is defined (if rather selectively) as a violent confrontation between modern, industrialised states using organised armed forces, can we imagine that cyberspace could prove to be an environment in which war begins, is fought and concludes decisively, with victory for one side and defeat for the other? Richard Clarke, US National Security Council Coordinator for Security, Infrastructure Protection and Counter-Terrorism under Presidents Bill Clinton and George W. Bush, has long been known for his pessimistic (some have said alarmist) perspective on the risk of conflict in cyberspace. In Cyber War, published in 2010 Clarke and his co-author Robert Knake insisted that 'Cyber war is real' and described cyberspace as 'a war zone, where many of the decisive battles in the twenty-first century will play out… What the United States and other nations are capable of doing in a cyber war could devastate a modern nation.' In 2013, in his unequivocally entitled Cyber War Will Not Take Place, the scholar Thomas Rid was deeply sceptical of what he saw as exaggerated and doom-laden visions of this sort, urging his readers to move beyond the 'tired and wasted metaphor of 'cyber war''.

2. For the time being at least, the evidence would seem to support Rid's argument – there has not yet been a confrontation in cyberspace that could conform to the definition given above. That does not, of course, rule out the possibility that at some point in the future cyber war (as defined) will take place. And in any case, Clarke's argument is also supportable, insofar as there has been more than enough evidence that cyberspace is indeed being treated as a 'warzone' (of sorts) in which 'battles' (of sorts) are being fought between states and sometimes with non-state adversaries, albeit without (so far) proving to be 'decisive'.

3. Is 'cyber war' nothing more than an empty, overused metaphor? Certainly, the expression is voiced in a very wide range of circumstances, many of which would appear to have very little, if anything to do with violent confrontation between states and other organised actors in the international system. Yet it is a particularly evocative and resonant expression, one which captures the imagination in the public debate. At the time of writing this report (October 2018) 'cyber war' and even 'new cold war' were in frequent use to describe certain opaque and sinister activities alleged to have been undertaken by the Russian state in the UK and elsewhere. And this is surely the point of metaphor; reference to the familiar and the comprehensible in order to describe and explain what is unfamiliar and complicated.

4. A more productive discussion might instead be had about the slightly different, and lesser prospect of cyber warfare – the organised use of armed force (and other levers of national power) for political purposes, where states might find themselves in conflict with other states or with non-state actors (e.g. terrorist, extremist and organised criminal groups), in which a decisive outcome might not be appropriate, necessary or possible. This is otherwise known as the 'fifth battlespace' argument in which cyberspace is understood as a new but not entirely separate component of a multifaceted conflict environment which also includes land, sea, air and space. By this view, cyber warfare is more a description of operational activity (by armed forces, intelligence agencies, law enforcement bodies and others) than it is shorthand for decisive strategic confrontation.

5. There is no shortage of metaphors and descriptors for what is taking place in cyberspace: ‘cyber war’; ‘cyber warfare’; ‘hybrid war’; ‘new generation warfare’; and ‘nonwar’. In his book The Virtual Weapon (2017), Lucas Kello provides an unusual addition to the lexicon with the term ‘unpeace’, defined usefully as ‘mid-spectrum rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition and possibly, even, of war.’ But our preoccupation with terminology might be missing the point. That point, surely, is that under whatever name we choose to describe them, military operations (loosely defined) are taking place in cyberspace. And the very fact that the relative merits of these terms are being discussed with such solemnity could distract us from the more important challenge of analysing, understanding and, above all, managing what is now taking place.

Is cyberspace a battlespace?

6. Is cyberspace somewhere – or something – in which armed conflict could take place? Does the prospect of conflict in cyberspace transform, or even revolutionise our thinking about strategy, warfighting and military operations; thinking that has evolved over centuries? Or is this supposedly novel challenge one with which we have long been familiar, in the form of information warfare, electronic warfare and, latterly, so-called hybrid warfare? As ever, the truth lies somewhere between exaggeration and complacency. We should not assume that cyberspace changes everything in the military sphere, and neither should we complacently confuse ‘hybrid’ with ‘cyber’. Warfare has probably always been ‘hybrid’ in some respects, but cyber operations are more than a modish, 21st century illustration of traditional military practice. Hybrid warfare is a strategy, but it is not a terrain. Cyberspace, on the other hand, can usefully be described as a ‘conflict terrain’; it is a medium of conflict. After all, if cyberspace is not ‘somewhere’ then it might make little sense, in the context of the territorially-preoccupied North Atlantic Treaty, to speak of triggering the Article 5 mutual defence clause.

7. Conference participants heard that armed forces’ understanding of cyberspace is evolving; armed forces now consider that with appropriate tools and techniques, cyberspace can be exploited to help achieve tactical, operational and strategic effect. Much of this activity would be supportive of conventional military operations: command and control; reconnaissance and situational awareness; operational and tactical planning; and logistics and supply. But as these supporting activities are, as they have always been, essential to the military effort, so they are themselves targets for attack (whether conventional or cyber). In other words, whether by design or simply through practice, cyberspace has indeed become a battlespace, a ‘domain’ of military operations. Some would disagree. By one view, although the term ‘domain’ resonates with a military audience, it is the wrong word – we should instead think of cyberspace metaphorically as a substrate; a surface or layer on which an organism can live and grow. By another view, since cyberspace touches upon all of human activity, it might be more accurate to describe it as a ‘super-domain’, inviting further discussion about where the boundaries might then lie between military and civil responsibilities and between types of military activity.

8. Whether substrate or domain (‘super’ or otherwise), within the cyber dimension – as in all other dimensions of warfare – the high-level goal must be to maintain ‘freedom of manoeuvre’. In this minimal sense, the ‘cyber battlespace’ does not appear to change the way wars are fought, it simply extends or modifies existing military practice. ‘Freedom of manoeuvre’ reduces to two requirements: freedom of action and freedom of decision-making. These requirements are not new, and so we should expect to see traditional military operational planning and language being applied in the cyber battlespace just as we would in any other domain of armed conflict.

9. In other respects, however, cyberspace is far from being a standard or traditional environment for military operations. Cyberspace blurs the boundaries of time and geography that have long constrained military operations. Equally, the use of cyberspace as a vector for asymmetric warfare challenges the boundaries of what constitutes an appropriate and effective use of armed force, and what does not. But this uncertainty can be turned into a strength – or at the very least can become a distinctive feature of our approach to operations in cyberspace. The fact that most cyberattacks on NATO, for example, have taken place below the threshold of a traditional, conventional armed attack, suggests that there must be a commensurate, i.e. non-military response at that level.

10. The cyber battlespace is not therefore an exclusively military responsibility; there must be effective orchestration of civil-military capacity if cyberattacks – at whatever level and of whatever sort – are to be deterred and defeated. Military operations in cyberspace, however distinctive they might appear, must nevertheless be 'fought' as part of a comprehensive, integrated civil-military approach in which civil and military efforts are interdependent and more effective as a result. Civil-military co-operation is not new either, but it is no longer optional and so we can expect to see ever closer and more rapid integration (or what the UK government refers to as 'fusion') of civil and military agencies in the deterrence of, and response to cyber aggression.

Conflict prevention, confidence building and deterrence

11. Conflict prevention, confidence building, and deterrence are among a range of ideas, tools and strategies that reached their maturity during the decades of the Cold War. If we are interested in preventing conflict in cyberspace, and in reducing the need for military operations in that substrate (or domain, or dimension), then it seems reasonable enough to ask whether these highly-evolved, Cold War mechanisms might also be effective in the cyber environment. They might, but only after careful thought and adaptation; these ideas and protocols were formed in the peculiar circumstances of the Cold War and should not be expected to survive in a new environment without careful nurturing.

12. The purpose of conflict prevention is to reduce unpredictability and to emphasise the management of delicate, tense or deteriorating situations over the reaction to unexpected crises for which little or no preparation has been made; a high-risk situation that might result in costly – and avoidable – conflict. Hence the interest in mediation, a classic tool both of conflict prevention and conflict management (discussed later in the conference). In the cyber environment, however, the difficulty with early mediation is that it requires parties to a 'tense situation' to identify themselves as such. If they are to be effective, conflict prevention and mediation require a substrate formed of transparency, trust and communication, all of which, unfortunately, can prove to be scarce commodities in the era of 'plausible deniability'. Finally, conflict prevention and mediation also require early warning and preparation time if they are to be effective, whereas a cyber crisis might develop in a matter of minutes and hours rather than days and weeks.

13. Might confidence building measures (CBMs) – another echo of the Cold War – be useful in establishing some of what is needed for conflict prevention and mediation to take hold? Regional organisations such as the ASEAN Regional Forum, the Organisation of American States and the Organisation of Security and Cooperation in Europe have all considered the value of CBMs, with the latter producing, in 2016, a list of no fewer than sixteen CBMs designed for states to 'reduce the risks of conflict stemming from the use of information and communication technologies'. The purpose of CBMs is to generate a transparent, co-operative climate in cyberspace, making interaction less unpredictable and making it possible to understand and anticipate an adversary's or competitor's motives. But CBMs are not a prime mover – they depend for their success upon the political support of the respective governments, whether bilaterally or as members of a regional organisation.

In the case of the OSCE, with arguably the most developed regional approach to CBMs in cyberspace, that support is at present lacking. The Cold War also saw the evolution of a more ambitious form of CBM, intended not merely to encourage transparency and confidence but in addition to produce security – CSBMs, in Cold War parlance. When circumstances are conducive, CSBMs can make a very significant contribution to stability and conflict prevention; the 1972 United States-Soviet Union Incidents at Sea Agreement is often cited in this regard. If they are to succeed, however, CSBMs require mutual self-restraint among adversaries and competitors; a commodity which, again, is too little in evidence in cyberspace at present.

14. The final option to be considered on the list of conflict prevention options is deterrence; on the one hand a feature of human interaction for as long as humans have been interacting, and on the other hand the most strategically, technologically and psychologically sophisticated legacy of the Cold War. The underlying idea of deterrence is straightforward; it works by promising to impose costs on a given action, either by making success more difficult or by threatening a punitive response. The perpetrator, if acting rationally, should then be convinced that the benefits of the action will be outweighed by the costs incurred or the punishment received, and will then choose not to act as intended.

15. It follows that the purpose of cyber deterrence should be to convey the message that the benefits expected from adventurism or aggression will be outweighed by the costs and/or punishments imposed. Understood in this way, effective cyber deterrence would be a strategic posture combining both passive and active elements; cyber deterrence would require the capacity both to resist and to respond. But this is merely to transplant the language of one strategic era and environment (20th century Cold War) to another (21st century cyberspace) with little of the careful nurturing mentioned earlier. One participant observed wryly that ‘a cottage industry on cyber deterrence’ has established itself in recent years. If that is so, then this industry’s workforce must do more than simply repackage old ideas; it should delve more deeply into how a cyber variant of deterrence could prevent conflict in cyberspace and set the conditions for cyber détente.

16. Cyber deterrence poses difficult questions. Should we expect both components of traditional deterrence (‘denial’ and ‘punishment’) to operate with equal emphasis and equal effect in cyberspace? Or is it the case that denial (more commonly known as ‘resilience’ in the cyber era) will be the dominant, albeit passive feature of cyber deterrence? If that is the case, how active and responsive should we expect cyber deterrence to be? Does the Cold War model of strategic deterrence leave us with the expectation that cyber deterrence should be mainly, if not exclusively, a national military concern? If so, how can we mitigate that tendency, ensuring that we take the fullest account of a state’s cyber deterrence capability – much of which will be non-military, and much of which will not even be owned by government? The private sector is no longer merely the provider of deterrence capability to the government, as it was during the Cold War; it is a deterrent actor in its own right, with its own interests to protect and its own conflicts to prevent. The Cybersecurity Tech Accord and the Global Cyber Alliance, for example, bring a fresh, non-traditional perspective to the stabilisation and security of cyberspace, including the concerted exposure of malicious actions and actors as a form of ‘civic deterrence’.

17. How can we ensure that the private and public sectors collaborate to best effect? And if the public sector cannot be expected to be solely responsible for cyber deterrence, what is it reasonable to expect of government? The conference learned of the US Government’s efforts at a ‘fundamental rethinking’ of the deterrence of ‘malicious cyber activities’, of ‘destabilising state conduct in cyberspace’ and of ‘malicious non-state actors’. The deterrence of cyber-attacks that would constitute a use of force remains relatively straightforward – the traditional combination of denial and

punishment. But where malicious activity falls below the threshold of the use of force, a more nuanced position is called for. One proposal under discussion within the US Government is for the development of a 'menu of options for swift, costly and transparent consequences below the threshold of the use of force.' Developed on an interagency basis, this menu of consequences would be discriminatory and proportionate and in some sense adversary-agnostic, unlike the more bilateral/relational models of Cold War deterrence. The menu would also be sensitive to the need to manage any risk of escalation.

Cyber weapons

18. If and when preventive measures fail, what are the means with which a cyber conflict might be fought? What are 'cyber weapons'? Who invents them, and for what reasons? How can cyber weapon-related innovation, the weapons themselves and their effects, all be controlled, and by whom? At its simplest, a cyber weapon (much like any other weapon ever invented) is a combination of opportunity and technology, followed by action and effect: the opportunity amounts to the discovery of a bug, flaw or vulnerability in an ICT system; the technology required is a combination of exploit (software designed to use the flaw to gain unauthorised access to that system) and malware (software designed to disrupt or damage the system and its user[s] and/or to generate further effect); action involves the deployment of the exploit in the right place and at the right moment in order to infiltrate the malware; and the effect could involve everything from loss of personal data to temporary network disturbance, industrial espionage, election manipulation, network collapse and indirect physical damage. By some accounts, the latter could even be on a scale comparable to the damage caused in a nuclear attack.

19. As with so much of the discussion of cyber war or warfare, however, while the familiar language of national strategy can be used to describe cyber weapons and their uses, it does too little to explain the broader challenges they present. If we aspire to control the development, proliferation, use and effect of cyber weapons, then we must first find a way to classify them. Yet classification is not a simple matter. Some 'weapons' are exclusively military, others are what was formerly known as 'dual-use' (i.e. having both military and civil applications) while others are entirely civil technologies. Others are not obviously weapons at all; they might be vulnerabilities in some otherwise innocent part of the national infrastructure (usually privately owned) which can be 'weaponised' in the sort of attack described above. Some of these weapons could be classified as 'kinetic' (i.e. having physical effect of some sort, including damage) while others are better understood as 'cognitive' (i.e. information tools used in election manipulation). Innovation in this field is also very largely civil-led, rather than the product of highly classified research in government-owned laboratories.

20. For these reasons it would certainly be strategically and technologically ambitious to attempt a cyber equivalent of arms control, whereby the manufacture, possession and use of cyber weapons would be carefully managed, ideally with the mutual consent of interested governments together with other stakeholders in the private sector and elsewhere. It might also be strategically inappropriate, premature and risky to make such an attempt. The character of cyber weapons continues to evolve, as does the balance between offence and defence in cyberspace. It would be reasonable to suppose that possession of cyber weapons in some form would be necessary for the credibility of in-kind (i.e. cyber) deterrence. But even if a government were to renounce the possession of an offensive capability for deterrent purposes it would still be expected to defend itself against cyber-attack which in turn would require at least a working familiarity with current developments in cyber weaponry. In the view of one participant, cyber defensive capabilities are some five years behind the level of maturity of offensive capabilities. It is not clear, therefore, why at this moment any cyber-capable government would embark upon an 'e-arms

control' programme, the effect of which might be no less than to limit its own offensive (and deterrent) capability.

21. The challenge of cyber weapons is more complex than simply ensuring that national armed forces have the means to deter, defend, fight and win. The challenge to acquire cyber weapons is very strong, while the incentives and procedures to control them are weak. We find ourselves in an 'insecurity dilemma'. Two questions arise, the first of which should be of immediate concern for governments and national armed forces: how can cyberspace be made more stable while governments and armed forces are unwilling (often for good reason) to forego certain capabilities? The second question should concern governments and the private sector: where security, defence and resilience are concerned, how can the weaponization of national assets be prevented, especially when these assets are privately owned?

Justification of military operations in cyberspace

22. The fourth session of the conference turned to political-strategic justifications for the recourse to military operations in cyberspace. The spirit of the Prussian General Carl von Clausewitz walked the room, urging the conference to consider the bases upon which national and alliance leaderships might contemplate military activity in cyber space, and with what purpose. Before they can make such a judgement, Clausewitz would expect today's strategic leaders to be fully aware of what is taking place in cyberspace, where the threats, risks and vulnerabilities lie, and to be clear in their deliberations as to how (and how effectively) military operations could meet these challenges.

23. The accepted wisdom is that spending on cyber operational capabilities is increasing around the world. It is also generally accepted that a growing proportion of that spending is being committed to the development of offensive cyber capabilities, with perhaps as many as 50 countries already possessing such means. Should this be a matter of concern? Are we in the midst of a cyber arms race of some sort? Since, as we have seen, it is not an easy matter to distinguish between 'offensive' and 'defensive' where cyber capabilities are concerned, it would be difficult for strategic leaders to judge whether cyberspace is tending towards stability or instability. This points to a broader problem. The strategic discourse readily draws upon concepts of arms race stability and crisis stability when contemplating cyber warfare. But perhaps too readily; after all, these are concepts born of the very particular circumstances of the ideologically-driven Cold War. This is not to suggest that the Cold War was all about confrontation – there was, of course, adversarial co-operation and détente – nor that strategic stability is not a reasonable aspiration in the post-Cold War era. In Syria, for example, Russian and US forces understand each other's position and intentions well enough to avoid errors and miscalculations. The point here is that the Cold War was a deep, ostensibly irreconcilable, ideological confrontation which created the need for such highly-evolved ideas as arms race stability and crisis stability; these ideas did not exist before the Cold War, at least not so explicitly and deliberately, and it is not necessarily the case that they will apply easily to the post-Cold War prospect of conflict in cyberspace.

24. To some extent, strategic concerns about conflict in cyberspace reflect anxiety that such conflict could exacerbate strategic uncertainty elsewhere; of which there seems to be plenty. Normative prohibitions against the use of weapons of mass destruction are crumbling. The boundary between nuclear and non-nuclear weapons is becoming more porous as leaders in more parts of the world embrace the primitive, mid-1940s notion that atomic and nuclear weapons are simply 'bigger bombs'. This is not a climate in which unjustifiable or badly-managed military operations should be allowed in cyberspace, if the result is to precipitate broader conflict. And then there is what one participant referred to as the 'connectivity paradox'. Whereas during the Cold

War it was assumed that technological supremacy would equate to strength and safety, in the digital era, as the most technologically sophisticated countries become ever more cyber-dependent, technological advancement has had the opposite effect, with those societies becoming disproportionately vulnerable to cyber-attack.

25. Military agencies such as the Main Directorate of the Russian Armed Forces (GRU) and the Third Department of the Chinese People's Liberation Army (3PLA) are known to be very active in cyberspace. But these activities concern intelligence-gathering and espionage rather than conventional military operations. Strategic leaders must give careful thought to what they could expect of conventional military operations in cyberspace. In the first place, armed forces might be expected to do in cyberspace what they have always done in other domains – defend. But this will not be an easy request to make, given that so much of the malicious activity that occurs in cyberspace takes place at a level below the threshold at which the use of military force would traditionally have been justified.

26. In cyberspace, the balance of initiative and capability tilts strongly in favour of the offensive over the defensive. Defensive preparations might not therefore be sufficient and so perhaps the armed forces might be expected to carry out their historical function of 'taking the fight to the enemy'. This willingness to project force counter-offensively, and in a measured and proportionate manner, could also serve another function – that of strengthening a deterrent posture. But given uncertainties over the means, methods and purposes of military operations in cyberspace, perhaps a more straightforward test should be applied, one that is more prophylactic than practical; to stabilise the strategic relationship and to control vertical and/or horizontal proliferation.

The conduct of military operations

27. Will military operations extend into cyberspace, or will cyberspace define military operations? The possibility of 'continuous strategic campaigns' in cyberspace suggests not only that military forces will increasingly be called upon to meet political objectives in cyberspace, but also that cyber operations will in some form become a component of all military activity, in all domains. The sense of the conference was that however pervasive, cyber operations would not overwhelm the traditional military function; cyber operations must be 'normalised' across the military environment and will come to be viewed as ancillary to mainstream military operations, as with electronic warfare and signals intelligence.

28. Yet the prospect, if not the inevitability of military operations in cyberspace might have implications for the hierarchy of military effort known as the 'levels of war'; the tactical, the operational and the strategic. The operational level of war has traditionally been understood to be a connecting device; the point at which tactical effort is co-ordinated and organised in order to create options at the strategic level. In the era of pervasive cyber operations is this hierarchy still relevant, or will all military activity in cyberspace, on all levels, become more homogeneous, with cyber activity running as a single thread from bottom to top? If so, there might be implications for military command structure and, more importantly, there might be enduring structural consequences for the politico-military relationship. The operational level has not only served to connect, it has also served as a separation device, ensuring that activity at the tactical level is not pulled up into the strategic environment. If cyber conflict blurs the levels of war then there is a risk that clarity will be lost as to where and by whom policy/strategic decisions are made, who informs those decisions and who carries them out.

If future crises can be expected to have a cyber component then it is likely, to say the least, both that the military will be the target of very fast-paced cyber-attacks and that they will be required to contribute to national security and defence in cyberspace. To satisfy these defensive and counter-offensive requirements, from 'day zero' of a cyber conflict armed forces will need enough practitioners with the aptitude for cyber operations. These practitioners will need to have been trained at the highest level on specialist cyber ranges using the technology they would expect to use in conflict. That technology might include digital techniques for camouflage and concealment of critical networks and perhaps a stock of zero day exploits ready to be deployed against an aggressive adversary. Military leaders and practitioners will also need to be aware that the adversary is unlikely to sit back and do nothing. Too often, cyber exercises or 'war games' are centred on capabilities, taking too little account of what an adversary's intentions and, most importantly, its responses might be.

29. The environmental characteristics of cyberspace do not differ between land, sea, air and space. The need (and the opportunity) for military operations in cyberspace to be conducted as a joint (i.e. inter-service), collaborative effort should therefore be self-evident. With the political and military uncertainties that are likely to be a feature of military operations in cyberspace there will be a need for robust command and control procedures if that joint effort is to be as coherent, timely and effective as it can be. And as in other areas of joint military operations there will be a need for a doctrinal framework to guide training and preparation and for a system of joint 'battle damage assessment' to review operations, identifying successes and failures in order to inform future operations.

30. Joint doctrine, preparedness and training will also be essential at the allied level, ensuring that different national activities complement each other, rather than create confusion, misunderstanding and entanglement. NATO, for example, has recognised cyberspace as a domain of conflict while at the same time acknowledging, in the words of the Alliance's Secretary General, that 'nowhere is the fog of war greater than in cyberspace'. In NATO's case, the prospect of allied military operations in cyberspace often invites discussion of the Alliance's mutual defence clause (Article 5 of the Atlantic Treaty); whether and when it would be invoked or 'triggered' by a cyber-attack. The conference heard that Article 5 is more nuanced than is generally supposed. Cyberspace does not present an impediment to the invocation of Article 5, but that invocation would be neither automatic nor immediate. An Article 5 response need not be military and need not match the scale or style of the attack. There are no 'red lines', in other words; Article 5 decisions will be made by consensus and on a case-by-case basis by the North Atlantic Council, the Alliance's political leadership.

31. Interoperability at the allied level could very well include non-military agencies; the European Union's Cyber Diplomatic Toolbox could be used to curtail malicious behaviour in cyberspace. The value of the mixed, civil-military response is also understood within national governments. In the UK, for example, military operations in cyberspace should be considered as but one element of a full-spectrum, cross-governmental strategic approach that has recently come to be known as the 'fusion doctrine'. One participant thought in terms of a sliding scale, running from operations that are wholly military in conduct and effect; to military operations that might have a non-military effect (or a mix of military and non-military); to activity that is purposefully non-military in appearance, conduct and effect. It is then possible to understand the important distinction, at the national level, between narrow and broad strategies for cyber warfare. The first of these is more weapon-oriented (kinetic and otherwise) and might be considered the exclusive concern of the military. The broad strategy, however, considers national objectives in cyberspace in the round, and asks how military operations can support those objectives. Whether the strategy is narrow or broad, the political leadership will at all times require advice from military commanders as to what military operations can and cannot achieve in cyberspace.

Conflict management and conflict mediation

32. With our notional conflict firmly underway, the attention of the conference turned to the mediation and management of a 'live' conflict as opposed to its precursors, and to the means of ensuring that military operations in cyberspace would not result in an escalation of the conflict, whether in cyberspace or conventionally/kinetically. A number of problems soon presented themselves.

33. In the first place, when conflict takes place above the threshold of the use of armed force, military operations very soon begin to follow their own logic, not unreasonably, and military priorities can take precedence over mediation which might be regarded as 'having had its moment' in the pre-conflict phase. 'Self-help mediation' – e.g. the use of hotlines between adversaries – might not be considered useful at this stage. The second problem is that mediation, if it is to be attempted during conflict, requires a level of trust between the parties to the conflict, and the willingness and means to communicate. The problem in a cyber conflict is that the means of communication might also be the platform being used for attack (and defence). Other than bilateral communication, other, more orthodox ways to mediate might have to be considered, such as the good offices of international organisations or other third parties, and perhaps industry-led initiatives of various sorts. The scope for mediation will largely depend upon the level and urgency of the conflict and on its propensity to escalation.

34. Escalation poses yet more challenges. In the first place, we have little experience of de-escalating a conflict in cyberspace, particularly when that conflict is characteristically multi-level, involving ideational, policing, security and economic dimensions. The multi-level complexity of cyber conflict results in 'cyber insecurity dilemmas', in which it is difficult to see how escalation can be controlled, and by whom. Another challenge is that unlike deterrence, a strategy of compellence might first require escalation to take place in order to make a coercive case for de-escalation. In the opaque yet very fast-moving circumstances of a cyber conflict it might therefore be difficult for strategic leaders and military commanders to know when to escalate and when to de-escalate. This suggested to some participants that we might be in the grip of an escalatory cycle from which there is no escape; a 'tit-for-tat' dynamic with no prospect for mediation and resolution. Some then questioned whether it was at all appropriate even to consider mediation while under attack, as is arguably currently the case; governments become interested in mediation when they are losing a conflict and need to sue for peace. Rather than accept defeat, for the present it might be preferable to admit that escalation without end might be necessary. Yet if mediation of cyber conflict is neither possible nor preferable then, as one participant observed drily, we find ourselves in a stark position.

Constraints on military operations – ethical and legal

35. If conflict cannot be prevented, mediated and resolved then surely it must at least be constrained in its conduct and its consequences. Ethical principles and legal prohibitions have evolved over centuries with precisely that goal in mind. But if the means, modalities and purposes of military operations in cyberspace are as elastic as they seem, then how straightforward will it be to apply these constraints? More to the point, is cyberspace so opaque and unfamiliar that these high-minded frameworks – legacies of our analogue past – will simply never find purchase in cyberspace? If the 'road to war' could now last minutes, rather than months, how much time can be expected for ethical reflection and legal deliberation?

36. Keeping ethics out of policy and strategy for cyberspace might not be an option, however. In the first-place politicians, civilian officials and military officers might well have a moral conscience that should inform the decisions they take. Even if they do not have a conscience, the public and the media will have their own, thus narrowing the possibility of an 'ethics deficit' in public policy and national strategy. There is a need for a common moral lexicon since that is the basis of trust and, in turn, the basis

37. of a productive discussion about the sort of laws and rules that will be needed to govern operations in cyberspace. The ethics of war have also evolved as a sophisticated tool of assessment, one that can help to penetrate and understand the cyber fog. Metaphors do need to be used with care, but they can be useful. 'Cyber war' might seem aggressive, but if its outcome is death and destruction then it might be reasonable for it to be considered merely a variation upon a theme we have known for centuries.

38. If cyber 'action' or 'operations' – which might include a deliberate, disabling attack on a country's civilian infrastructure – are only analogous to 'war' then the just war tradition – and all that is derived from that tradition – might not apply concretely and we might need to find other ways to describe and evaluate what we see. On the other hand, if 'cyber war' is an accurate descriptor then the ethics of war are valuable insofar as they remind us that war should serve a purpose higher than itself. The means must serve the end, rather than vice versa; war should be ordered and disciplined in such a way as to serve a 'just peace'. Just war ethics also introduce the principle of proportionality, vital if organised conflict is to serve a higher goal and if we are to ensure that the damage caused is no more than is necessary to achieve the just peace. The proportionality test should also be applied to defensive postures and actions, the purpose of which should be to convince an aggressor not to persist. Finally, the just war ethical tradition can assist with targeting decisions; harm or damage to civilians or non-military objects can be admissible if these people (including computer scientists, perhaps) and objects are associated with a legitimately targetable infrastructure or if the harm inflicted is unintentional.

39. Although military operations in cyberspace are a new twist in the human experience, as with the ethics of war it does not follow that the international law of armed conflict (LOAC) has become irrelevant and should be rewritten. But neither, conversely, will the application of international law to military operations in cyberspace be a straightforward matter, for several reasons. First, international law begins from the premise of permission, rather than prohibition; actions (including those taken by military organisations in cyberspace) are permitted unless they are expressly prohibited. Second, LOAC would apply only if the threshold of armed conflict has been crossed, inviting debate as to whether, and when, a 'cyber war' could be said to have crossed that threshold. Third, the principles of distinction and proportionality – imported into international law from the just war tradition – apply to a military force when it is attacking (whether in the offence or the defence), but not when it is carrying out actions that fall short of attacks. Since much of what might be undertaken in cyberspace might not constitute an attack, as traditionally understood, then even if cyber operations were to be directed deliberately against civilians and civilian infrastructure (e.g. an action against a city's power grid), or if civilians were the target of non-violent actions such as propaganda and misinformation, the LOAC principles might not apply.

Constraints on military operations – ethical and legal

40. The penultimate session of the conference asked how military operations in cyberspace might be concluded, and how we would know when peace and stability had been restored. In particular, what would 'cyber victory' look and feel like? And conversely, what would it mean to lose a cyber conflict?

41. The military mindset is concerned with decisive action leading to decisive outcome. By one view, however, a cyber conflict is unlikely to produce the unequivocal and durable results that might traditionally have been expected of military operations. Instead, a more nuanced understanding of 'cyber victory' should be sought by thinking tangentially and analogically. As is the case whenever armed forces are deployed operationally, the first step in the evaluative process should be to remind ourselves of the higher strategic aim, and then to ask how the different components

of a military operation would serve that aim.

42. Coalition operations against Da'esh, for example, resulted in victory in that the proto-state was largely defeated militarily. That defeat was achieved through a form of attrition warfare, steadily reducing the number of fighters available to the Da'esh leadership. Cyber operations made little direct contribution to the campaign of attrition, yet they did contribute significantly to the campaign against the Da'esh ideology, and that in turn helped to undermine the Da'esh fighting spirit.

43. Others were not convinced that modern armed forces could adapt to and exploit the new environment, arguing that even the most capable armed forces could be subjected to complete and total defeat within minutes. If military operations – defensive and offensive, in cyberspace and generally – could be disabled in this way then the 'military mindset' referred to above, premised on the notion that decisive action can have a decisive influence on victory and defeat, is worryingly close to becoming a quaint legacy of the military past; no more relevant to cyber warfare than the infantry squares at Waterloo are to modern counter-insurgency warfare.

44. Another way to judge the effectiveness (and cost-effectiveness) of cyber operations might be by analogy with a blockade, whereby unsustainable strategic and economic costs are imposed upon an adversary. But the imposition of cost is rarely, if ever, unidirectional; the institutions and mechanisms with which these penalties could be imposed do not come without charge. In the United Kingdom, for example, the establishment of the National Cyber Security Centre has been at significant expense. These expenses must be included in a comprehensive cost/benefit assessment if victory (e.g. against Da'esh) is not to be achieved at disproportionate cost.

45. The costs of victory might be felt in other ways, particularly when the conflict is judged to be something less than a fight for national survival. It might prove difficult to maintain political and strategic cohesion, at both national and alliance or coalition levels, and it might also be that specific sectors of society (such as the finance and banking system, for example) might find it damaging to be used as a tool in strategic coercion. It should also be borne in mind that we know too little of cyber conflict to be able to predict with much confidence the wider consequences of military operations in cyberspace. There are likely to be unintended and unforeseeable consequences of cyber conflict, with a digital version of 'collateral damage' being felt widely, deeply and long into the future on all sides of any cyber conflict. Perhaps, therefore, no country should contemplate military operations until it has established large-scale societal resilience to cyber-attack; a socio-economic challenge on a very grand scale, and not one that armed forces can reasonably be expected to manage.

Futures

46. The Wilton Park cyber conflict having been brought to its conclusion, decisively or otherwise, the conference turned its attention finally to the future, and what it might hold for military operations in cyberspace. While we struggle to understand the political, strategic, economic and ethical character of conflict in cyberspace, and to distinguish between hazard and opportunity, it is sobering to consider that the technological advances of recent decades might prove to have been a slow start to a very fast-moving and disruptive phase of human history. The future might turn out to be anything but a comfortably linear projection from the present, one made more or less comprehensible by trend analysis, worst-case planning, war gaming, risk assessment, scenario and contingency planning, and so on. Instead, the pace and scope of technological change might be about to become exponential, complicating our understanding and management of the global cyber environment by several orders of magnitude. Curiously, the mere possibility that change might become overwhelming could already be influencing policy-makers and strategic leaders, constraining the security decisions they make. If technology might broaden the scope for offensive operations in cyberspace then we should also expect to see an equal

and opposite interest in defence and resilience. But since these technologies will have dual-use applications, both offensive and defensive, and since innovation is more civilian- than military-led, it will be important that any defensive posture remains adaptable to new threats and that current security priorities do not undermine that general capacity for innovation. In other words, policy-makers might find themselves being forced into taking more risk with current security than they might otherwise wish, in order to protect the capacity for innovation and to maintain strategic initiative in an uncertain future.

47. Other, more tangible challenges loom on the horizon. Perhaps the most pressing of these will be the strategic, technical and ethical management of autonomous weapon systems (AWS). Some see AWS to be the paradigmatic illustration of the exploitation of cyberspace for coercive purposes. But to what extent will 'operations' performed in cyberspace by AWS actually be 'military' in the sense that term has come to be understood, i.e. the closely supervised deployment of uniformed citizens organised into armies, navies and air forces in order to achieve explicit and justifiable political goals through the use of violence? It is not fanciful to suppose that the advent of AWS might herald the reordering of the relationship between society, government and armed forces.

48. Another challenge concerns the resilience of space systems. There are almost 2000 active satellites orbiting the Earth, forty per cent of which are for communications and another six per cent for navigation and positioning purposes. Roughly twenty per cent of all satellites are believed to have military uses. Many of these satellites – whether military or civil – are considered to be vulnerable to attack, such that the resilience of space systems, upon which society in general and armed forces in particular are becoming ever more dependent, cannot be assumed. Do we understand the security of outer space and cyberspace in a sufficiently integrated way? Could military or sabotage operations in cyberspace extend into outer space, perhaps even provoking a 'space war'? How could the source of an attack be attributed; what action should then be taken and by whom? As with cyberspace, most of this 'battlespace' is in the hands of the private sector, such as the privately-owned Inmarsat satellite telecommunications system upon which global shipping and airline industries depend. This brings into sharper focus the requirement for very close collaboration between the public and the private sectors. But it also invites further thought about the notion of resilience in this highly contested digital environment, more consideration as to how to win and maintain strategic advantage and deeper reflection on the cost that any such effort might impose on other sectors of society and the economy.

Conclusion

If 'Military operations in cyberspace' drew one lesson it is the need for intellectual, political and strategic humility. Our understanding of cyberspace as an environment, of conflict in that environment, and of the military role in such conflict are all still 'work in progress'. The conference invited further reflection on a series of intricate and urgent questions. In general, when contemplating conflict in or from cyberspace it would be wise to distinguish between what is familiar and what is unique about that prospect. If too much familiarity is assumed ('cyberspace merely allows the human propensity for conflict to extend into a new environment') then category errors might be made in applying the strategic templates and decisions of the analogue past to the different circumstances of the digital future.

Equally, to assume complete uniqueness might be to overlook the possibility that in important respects, 'we have been here before' (or somewhere nearby) and that there will be valuable experience to apply. Then there are questions to ask concerning the role of organised armed forces in such conflict. Is that role to fight, in the traditional sense of an action/reaction struggle with an adversary? Or is the military task to contain hostile

actions in cyberspace and to prevent them spreading to, and compromising military activity in the conventional domains (land, sea, air and space)? Might this defensive function be extended to society more broadly, with armed forces tasked not just to defend their own communications networks but also to ensure the resilience of society's critical national infrastructure as a whole? Could cyber defence and resilience be as much as should be expected of military deterrence in cyberspace? Or should the role of armed forces be more organisational than operational; a liaison and coordination function intended to ensure integrated cross-governmental and intra-alliance responses?

Whatever is expected of military operations in cyberspace, how should that activity be governed? Are democratic societies especially disadvantaged in this respect, by their inclination to interrogate the close detail of technological innovation, seeking to identify and eliminate any undesirable outcomes, while more authoritarian societies have fewer scruples? What, if any, should be the role of the private sector in the state's efforts to police, stabilise and defend cyberspace? Does international law for armed conflict need to be refreshed – or perhaps even revised – in order to take full account of military activity in cyberspace (particularly activity taking place below the threshold of armed conflict)? And what ethical boundaries should be set around and within military operations in cyberspace? Will it be sufficient, and even possible to apply the principles of discrimination and proportionality (born of the era of 'kinetic' armed conflict) to the digital battlespace? Finally, what can be done to ensure that these political, strategic, legal and ethical deliberations keep pace with technological innovation, the rapid phase of which might only just have begun?

Paul Cornish
Wilton Park | September 2018

Should you wish to read other Wilton Park reports, or participate in upcoming Wilton Park events, please consult our website www.wiltonpark.org.uk. To receive our monthly bulletin and latest updates, please subscribe to https://www.wiltonpark.org.uk/newsletter/