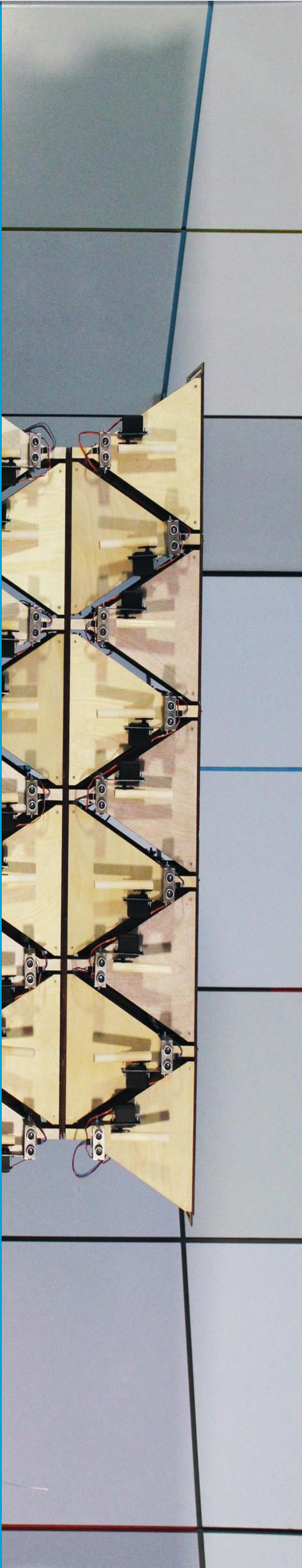
GLOBSEC

Future War NATO?

From Hybrid War to Hyper War via Cyber War



GLOBSEC NATO Adaptation Initiative

Supporting paper

GLOBSEC

The GLOBSEC NATO Adaptation Initiative, led by General (Retd) **John R. Allen**, is GLOBSEC's foremost contribution to debates about the future of the Alliance. Given the substantial changes within the global security environment, GLOBSEC has undertaken a year-long project, following its annual Spring conference and the July NATO Summit in Warsaw, to explore challenges faced by the Alliance in adapting to a very different strategic environment than that of any time since the end of the Cold War. The Initiative envisages a series of policy papers which will address the nature of NATO adaptation and the challenges it must overcome if it is to remain a viable and credible alliance for the peace and stability in the transatlantic area. The policy papers published within the GLOBSEC NATO Adaptation Initiative are authored by the Initiative's Steering Committee members: **General (Retd) John R. Allen, Admiral (Retd) Giampaolo di Paola, General (Retd) Wolf Langheld, Professor Julian Lindley-French, Ambassador Tomáš Valášek, Ambassador Alexander Vershbow** and other acclaimed authorities from the field of global security and strategy. The aim of the involvement of such a wide array of experts is to reinforce the unique partnership between policy-makers, military leaders and leading academics and commentators. These policy papers will prelude and result with the publication of the Initiative's Steering Committee Recommendation Two Pager and the Main Report to be launched in November 2017. The Interim Report will be released during the GLOBSEC 2017 Bratislava Forum.

These outputs will be augmented by shorter policy papers (on cybersecurity, A2/AD capability, intelligence, and threats emanating from the South) prepared by the GLOBSEC Policy Institute between January and October 2017.

Future War NATO?

From Hybrid War to Hyper War via Cyber War

Supporting Paper of the GLOBSEC NATO Adaptation Initiative

By General (Ret.d) John Allen, General (Ret.d) Philip M. Breedlove,
Professor Dr Julian Lindley-French, & Admiral (Ret.d) George Zambellas

"Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world".[1]

President Vladimir Putin
1 September, 2017

Abstract

This is a paper about NATO strategy in future war. It is built around two scenarios: one in which the Alliance is defeated because it did not prepare for future war; and another in which the Alliance prevails because it did. The paper calls for the crafting of a NATO Future War Strategy (and Strategic Concept) that would convince Moscow that under absolutely no circumstances would the threshold to war be so low as to make it imaginable, let alone winnable. Or, that the threat of such a war would force the Alliance and its nations to accept unacceptable compromises over either sovereignty or security.

Future war will see an adversary seek to destroy the ability of the Alliance and its nations both to protect people and to project power and influence in pursuit of sound defence. Future war will thus be part of a grand asymmetric strategy by enemies to offset Allied strengths. Attacks on Alliance societies will take place at the seams between peoples, their beliefs, and their states, to keep NATO strategically, politically, and militarily off-balance. Traditional military platforms, systems, technologies, and strategies, allied to new and accelerating technologies such as robotics, artificial intelligence and beyond, will be used in an effort to achieve decisive strategic aims quickly.

A NATO Future War Strategic Concept must be crafted to quickly establish a credible twenty-first century deterrence and defence, and forge the intelligent use of hard power with the smart use of technologies and influence across the conflict spectrum. Article 5 operations will need new ways to understand when an attack is underway and to establish rapid action, cyber-defence & offence, hybrid defence & offence, allied to the strengthening of societal resilience to address the attack. The Alliance must be able and willing to meet the force-on-force challenge from Russia and other adversaries. NATO is behind the twenty-first century future war curve, and adaptation must help that Alliance correct that.

[1] See, "'Whoever leads in AI will rule the world', Putin to Russian children on Knowledge Day". RT, 1 September, 2017. (N.B. This source can be relied upon when quoting the Russian President.) https://www.rt.com/news/401731-ai-rule-world-putin/

Future War NATO?

From Hybrid War to Hyper War via Cyber War

"We who have put this book together know very well that the only forecast that can be made with any confidence of the course and outcome of another world war, should there be one, is that nothing will happen exactly as we have shown here".[2]

General Sir John Hackett
The Third World War: A Future History
August 1985

Introduction

This paper is about NATO strategy in future war, and the fast-changing relationship between strategy and technology in warfare. Twenty-first century war will be a war fought with autonomous systems, in which mass disruption by an enemy could be the harbinger of mass destruction. How would NATO defend against such an enemy, and how would the Alliance fight and win such a war? The paper considers the interaction of Allied strategy with fast-emerging technologies, and the extent to which the former must adapt to the latter if collective Alliance deterrence and defence are to remain credible.

This paper calls for a new NATO Strategic Concept to address the challenges of future war. Several adversaries are engaged in preparing for future war, as is the United States. However, central to this paper is Russian thinking on future war. This is because Moscow has undertaken a systematic analysis of how an ostensibly weaker, but unitary actor, could exert influence over the far stronger, but far more divided, set of actors that is the NATO alliance. To that end, the paper rest on two scenarios: one in which the Alliance is defeated because it did not prepare for future war; and another scenario, at the end of the paper, in which the Alliance is victorious because it did.

The paper also considers Russian future war strategy as a case study in evolving strategic threat. The paper concludes with NATO's response, and the new balance the Alliance, its nations, and its partners must strike if they are to successfully protect vulnerable, open societies, and project the future warfighting power that will be vital to the maintenance of credible Alliance deterrence and defence.

The very idea of future war is controversial and must be acknowledged as such. Professor Sir Lawrence Freedman writes, "The idea that societies, and their associated military systems might be comprehended as complex systems encouraged the view, reflected in the perplexing searches for enemy centres of gravity that hitting an enemy system in exactly the right place would cause it to crumble quickly, as the impact would reverberate and affect all the interconnected parts".[3] In almost all imaginable circumstances NATO would not crumble and would respond. However, evidence from stated Russian strategy, and its military posture would suggest that President Putin, and some around him, actually believe a combination of Russian strengths and Western vulnerabilities might indeed afford Moscow such a 'decisive moment'. Or, at least, believe some strategic benefits might accrue to Russia, given that such thinking is now central to Russian grand and military strategy. Russia is already working on a range of strategies that support its belief that Moscow could benefit from what it calls

[2] Cornish P. & Donaldson K. (2017) "World of War 2020" (London: Hodder & Stoughton) p.2
[3] Freedman, L. (2013) "Strategy: A History" (Oxford: Oxford University Press) p. 239

"controlled chaos", in the event of a struggle with the West, that engages a range of media, technology and military assets to achieve strategic and political objectives.[4]

At best, the search for an accommodation with Russia must now be reinforced by the need to again consider the worst case. Whilst the West has undoubtedly made mistakes in its dealings with Russia, responsibility for this shift in Russian strategy and its aggressive posture must lie firmly with Moscow. Therefore, this paper is ultimately devoted to a NATO Future War Strategy that would convince Moscow that under absolutely no circumstances would the threshold to war be so low as to make it imaginable, let alone winnable, or that the threat of such a war would force the Alliance and its nations to accept unacceptable compromises over either sovereignty or security.

Core Message

The core message of this paper is thus: NATO needs a new Future War Strategic Concept if the Alliance and its nations are to maintain credible deterrence and defence in the twenty-first century. Specifically, NATO will need to have a far more holistic understanding of the relationship between protection of citizens and the projection of power and influence, in all its many forms. The Internet of Things, allied to emerging technologies with wide-ranging military applications, such as Artificial Intelligence, Big Data and the systems-driving algorithms it creates, make it increasingly possible for ostensibly far weaker powers, such as Russia, possibly in tandem with criminal and Islamist groups, to cause damage to Western societies out of all proportion to their size and capabilities. Such technologies will (and must) profoundly affect Allied security and defence policies and strategies, which are the focus of this paper.

Scenario 1:

Strat-Tech War 2025 - NATO Defeat in the Second Battle of North Cape

It is August 2025. The United States is mired in a growing short-of-war scenario that involves a series of dangerous crises in Asia-Pacific. Europe is vulnerable. Exhausted and worn down by the years of complex Brexit negotiations, sustained mass, irregular migration from its south, a seemingly endless flow of terrorist attacks, and years of relative economic decline caused by leaders unable or unwilling to take the necessary measures to resolve Europe's myriad political, economic and social tensions.

Britain's 70,000 ton heavy aircraft carrier *HMS Queen Elizabeth* is sailing off the North Cape of Norway. These are historic waters for the Royal Navy as 'Big Lizzie' is not far from where on the late afternoon of 26th December 1943, in the Arctic twilight, the British battleship *HMS Duke of York* sank the German battlecruiser *KM Scharnhorst*. The First Battle of North Cape was, in effect, the opening engagement of a new computer/missile age and the last battleship-to-battleship dual in history, in which no aircraft played any part.

By the standards of the age, *HMS Duke of York* [5]was a floating electronics platform armed with state of the art sensors and several layers of radar capability. The battle, most of which

[4] Gudrun Persson in a March 2017 article for the NATO Defence College critiquing a 2017 book, "The War of the Future: A Conceptual Framework and Practical Conclusions: Essays on Strategic Thought" by Igor Popov and Musa Khamzatov, that critiques Russian thinking and cites writes, "A particularly topical subject in Russian military strategic thinking in recent years concerns the view on soft power and so-called 'controlled chaos or manageable chaos…recent conflicts demonstrate that 'peaceful demonstrations, anti-regime demonstrations, and in some cases foreign military intervention turning entire countries and regions into a state of controlled chaos can now be called a new type of contemporary warfare". See Persson G. (2017) a critique of "The War of the Future: A Conceptual Framework and Practical Conclusions: Essays on Strategic Thought" by Igor Popov and Musa Khamzatov, (Rome: NATO Defence College) pps.5-6.

[5] Angus Konstam writes, that as well as "…the radars, the battleship [*HMS Duke of York*] was also fitted with an extensive suite of electronic equipment, designed to detect aircraft, radio or radar transmissions, IFF (Identification of Friend or Foe) transmissions from friendly aircraft or ships, and radar detection equipment. The battleship was buzzing with electronics, and although these were fairly rudimentary by modern standards, in late 1943 they were 'state-of-the-art', and that afternoon they were all working perfectly". See Konstam, A. (2009), "The Battle of North Cape: The Death Ride of the *Scharnhorst*, 1943". (Barnsley: Pen and Sword) p.113

took place in the Arctic dark, saw *HMS Duke of York* link her *Type 284* main gunnery radars to a rudimentary computer in the Gunnery Control Centre which then trained the ten 14 inch guns of the main armament. Unheard of in any prior battleship-to-battleship engagement, the *Scharnhorst* was straddled and hit by the initial salvo, with one main armament turret immediately disabled. The eventual sinking of the *KM Scharnhorst* some three hours later ended the threat posed by Nazi surface raiders to Allied convoys en route (and not without some historical irony) to Murmansk, Russia.

Tensions with Russia have been building for months as an increasingly erratic President Putin, faced with economic and societal challenges that makes those of the rest of Europe seem trivial, has become steadily more aggressive. Central and Eastern Europe face regular cyber-attacks, with banking, transportation, and even health systems effectively shut down for days at a time. RT, Sputnik, and other Kremlin-controlled Russian media organs, pump out increasingly hysterical fake news stories about Western aggression. In recent weeks, Russia's Western Military District (Oblast) has been reinforced with several new spearhead divisions, threatening much of NATO's eastern border. Worse, Russia has markedly increased both the number and type of treaty-legal and illegal nuclear weapons deployed to its Kaliningrad enclave between Poland and Lithuania.

Above the Arctic Circle the *Russian Northern Fleet* has adopted aggressive patrolling with aircraft, ships and submarines regularly attempting to intimidate NATO naval forces far out into the North Atlantic. However, the most dangerous encounters take place in the so-called Greenland-Iceland-UK gap, and close to Norway's North Cape.

In early July, Russia moved a large formation of Naval Infantry (marines) to Pechenga, close to Russia's short border with Norway. An alarmed Oslo called for Alliance support. On August 10th, as tensions ratchet up, and by way of response to Russia, the North Atlantic Council ordered SACEUR to take all necessary steps to demonstrate to Moscow the Alliance's determination to defend its borders, and the vital sea and air lines of communication around them. However, few US ships are available to the Alliance given the mounting tensions in Asia-Pacific, the size and capability of the Chinese People's Liberation Navy (PLN), and a series of humanitarian disasters in the Mediterranean and beyond, engineered by Russia and Iran, and partly linked to the ongoing migration crisis.

A hastily-organised NATO Task Group is formed and organised around *HMS Queen Elizabeth*. The Task Group includes ships, aircraft and submarines from Britain, Canada, France, Germany, the Netherlands, and of course, Norway.

August 15th 0430 hours: 150 nautical miles WNW of North Cape. Suddenly weapons and defence systems on board *HMS Queen Elizabeth* crash, as the Task Group flagship suffers a sustained cyber-attack, along with much of the rest of the twenty-ship flotilla. Almost simultaneously the huge ship is attacked by an intelligent swarm of autonomous, flying armed 'attack-bots'. The Second Battle of North Cape has begun.

0431 hours: Situational awareness is effectively reduced to nil. The decision-action cycle of the ship's captain is reduced to less than a second, whilst the commodore loses all communications and command and control links to the Task Group. Parts of the robotic drone swarm split up and attack specific systems on *HMS Queen Elizabeth*.

0432 hours: Internal communications are disabled and the damage control centre fails; the ship stalls to a sudden halt as the engines go into reverse. Two Russian *Yasen*-class nuclear attack submarines, successfully avoiding the 3G and 4G detection systems of the Task Group by exploiting the different temperature and density layers of frigid North Atlantic waters, each launch an *Iskandr PL* anti-ship missile and cripple 'Big Lizzie'. The damage to *HMS Queen Elizabeth* is devastating.

0434 hours: The ship takes on water rapidly and begins to list heavily to starboard. After an enormous internal explosion, a shocked captain gives an order he never thought possible. He orders the surviving crew to start shouting "abandon ship - every man and woman for themselves". Those 'lucky' enough to make it into the water die within minutes from hypothermia.

0453 hours: Twenty-three minutes after the attack begins, a burning *HMS Queen Elizabeth*, the largest ship ever to serve in the Royal Navy, capsizes and sinks by the bow, propellers spinning in the cold, dark, light of an Arctic dawn, with the loss of almost all hands. Much like *HMS Hood*, which blew up in the Denmark Strait in May 1941 not so far from the scene of the Royal Navy's latest battle, there are only three survivors from a crew of 1500. 'Big Lizzie's' complement of F-35 Lightning II/5 (Enhanced Range) fast jets, and Merlin 7 ASW helicopters, never got off her decks.

0454 hours: The Russian submarine *Novosibirsk* flashes a success signal to Moscow. It contains just one word; '*Kursk*'.

As 'Big Lizzie' sinks, vulnerable critical infrastructures crash across Europe. Telephone and computer systems fail, air and rail transportation is brought to a halt, TV and social media are hacked, and, through the Internet of Things, even certain domestic appliances begin to run out of control, some even exploding. Europeans awake to chaos. Disoriented, and in shock, they search for reassuring news only to find TV, radio and the social media suddenly seized with apocalyptic messaging warning of impending nuclear, biological and chemical attacks on major European cities.

Mass hysteria ensues. It is made worse by simultaneous terrorist attacks upon the gathering groups of bewildered people by sleeper cells carefully implanted into the European Union, most notably in Brussels where crisis response rapidly collapses. False reports of plague being spread by terrorists in several European city centres only complicate the movement of first responders and security forces as populations panic. Over the ensuing hours people try to flee Europe's cities, clogging up transportation arteries vital to any Allied military response.

Worse, political and military command in many NATO allies is rapidly decapitated at a stroke by a series of well-coordinated cyber-attacks on insufficiently robust government and military communications systems. NATO's limited forces are also over-stretched. Needed to reinforce the Enhanced Forward Presence in Eastern Europe, to cover an extended and continuing Russia 'Super Zapad' exercise, the bulk of NATO's main defence forces are covering the Baltic States and Poland. And, given the crisis in Asia-Pacific, available reinforcing US forces in Europe are few in number.

As the Second Battle of North Cape unfolds, and with Russian nuclear services on high alert, Russian forces seize Norway's North Cape, Spitzbergen, and all non-Russian forces within Arctic Circle. Moscow's aim becomes clear; to seize the new Northeast Passage between Asia and Europe and to secure by force all the hydrocarbons believed to lie under the Arctic Circle. With victory, President Putin becomes domestically invulnerable.

0930 hours: President Putin calls several NATO leaders and puts to them a simple, but brutal question, in his simple, but brutal way: "Russia's objectives have been achieved", he says, "and the threat to us removed." Putin continues, "Do you really want to go to nuclear war over some polar bears? I am ready, you are not. The British ship? That was regrettable, but NATO's deployment of HMS Queen Elizabeth was a provocative act and a direct threat to our Northern Fleet base. Our response was a proportionate and legitimate act of self-defence. By the way, China agrees. Ladies and gentlemen, we do not like each other. That is immaterial. I am offering you peace. After all, what price has NATO really paid and are you ready to consider the alternative?"

With NATO and the EU effectively disabled, 'solidarity' collapses. As dawn breaks on a cold, new reality questions begin to be asked of political leaders about the years of underfunding resiliency, readiness and response, both civil and military. One thing is clear; Europeans can neither protect themselves, nor can they project power. Welcome to the end of collective self-delusion. Welcome to strat-tech warfare.

A Twenty-First Century Pearl Harbor?

Could NATO suffer a twenty-first century Pearl Harbor? The December 1941 attack on Pearl Harbor took place in a vacuum between US policy, strategy, technology, and capability. The aim of broad spectrum holistic hybrid-cyber-hyper future war strategies is great effect at minimum time, and at minimum cost to its architects. At present, NATO, its nations, and most of the armed forces that serve it, are increasingly vulnerable to a crippling future war attack. In 2017, NATO faces a range of future war 'threats'. Interoperability within the Alliance is also becoming increasingly difficult, intensifying the vulnerability of open European societies and militaries to a range of crippling attacks. Adversaries such as Russia are systematically exploring those vulnerabilities and seeking to exploit them.[6]

Hyper warfare: The impact of new technologies, and the interactions between them, are changing fast the nature, character and conduct of war. Hyper war will see an accelerated speed of conflict allied to vastly shortened decision-action cycles. Hyper war will see an enormous compression of time and consequent effect, with the command of war becoming steadily and necessarily more automated; and part of a new escalation ladder that climbs from chaos to capitulation. The increasing reliance of Western populations on internet-based social media makes diverse societies vulnerable to political manipulation via fake news. This forms part of a new form of hybrid warfare which transcends the civil-military divide.

Cyber warfare: Cyber-based civilian infrastructures from healthcare to air transportation will also be natural targets, adding disruption of life to a profound sense of uncertainty. The threat of hyper warfare at the high-end of the military spectrum would simply ram home a message, by those who have mastered it, that resistance is futile.

One of the many dangers from such a hybrid-cyber-hyper warfare continuum is that it again renders plausible the once unimaginable idea of 'warfare' in and between developed societies. It could also render traditional nuclear deterrence, as a stand-alone stratagem of last resort, increasingly obsolete. Indeed, 'deterrence', as currently conceived of, will need to be re-thought across a new spectrum of conflict if it is to remain credible, whilst Allied armed forces will need to become demonstrably capable across many domains – land, sea, air, space, cyber, intelligence, information, and, above all, knowledge.

Russia and China are already making significant technical progress at the very highest-levels of future warfare, efforts that could soon be reinforced by new 'force multipliers', such as quantum computing and its integration into the future order of battle. There are concerns in the West that artificial intelligence in weaponry will produce morally unacceptable military capabilities. Quite possibly but, like the advent of the torpedo-firing submarine and the moral dilemma it created around commerce raiding on the high seas, the enemy will exploit any such capability 'freedoms'. Or, to put in another way, NATO is unlikely to successfully deter or defend against hybrid warfare unless it can also demonstrably do the same against cyber and hyper warfare.

Russia has placed increased emphasis on nuclear weapons, and other forms of unconventional hybrid and hyper warfare capabilities and capacities, to counter what Moscow believes to be NATO's conventional military superiority. However, such thinking about future war is not confined to Russia. Radical Islamist groups, such as Al Qaeda and ISIS, are also exploring the use of technologies and strategies to penetrate open, western societies, erode the protection of the home base, and undermine the social and political cohesion upon which all security and defence strategies in democracies must be based.

[6] In his 2016 book, "2017: War With Russia", former Deputy Supreme Allied Commander, Europe (DSACEUR) General Sir Richard Shirreff wrote, "It does not need Russian soldiers marching through Berlin and Paris for the world to as we know it to cease to exist. A militarily victorious Russia, able to dictate to a defeated Europe and NATO from the end of a barrel as to exactly what will and what will not be acceptable to them, will be enough for life as we know it in Western Europe to come to a very abrupt end". See Shirreff, Richard (2016) "2017: War With Russia", (London: Coronet) p. 13

Even the United States 'poses' a threat to Europe, at least to its complacency, after a decade of European defence cuts. Consequently, as technology increasingly drives and shapes both policy and strategy, a split is emerging between the US and Allied militaries. Indeed, technologically-driven US military strategy is advancing so fast compared with the European allies that, sooner rather than later, all-important NATO military interoperability might well become a thing of the past. Over time a profound mismatch in military technologies undermines the politico-military cohesion of any alliance.

Russia's strategic approach is technologically far less ambitions than its American counterparts, but robustly pragmatic. In effect, Russia is endeavouring to weave existing platforms, systems and strategies with new capabilities and technologies across the civil-military conflict spectrum. Critically, much like the British and German strategic bombing campaigns of World War Two, the Russians make no attempt to distinguish between combatants and non-combatants in a war that Moscow understands would be existential for the regime.

Russian strategy seeks to exploit and link technologies as a big power, short action strategy. It is a strategy which includes the threatened use of nuclear weapons to force an adversary to accept what Moscow calls the 'changing of facts on the ground'; gaining local military superiority via regional deployments and keeping adversaries politically and socially off-balance through the use of extended deception, thus rendering a cohesive defence impossible. The strategy is attributed to the long-serving Chief of the Russian General Staff, General Valery Gerasimov. In a well-known 2013, article General Gerasimov wrote, "I would like to say that no matter what forces the enemy has, no matter how well-developed his forces and means of armed conflict may be, forms and methods for overcoming them can be found. He will always have vulnerabilities and that means that adequate means of opposing him exist".[7]

Russian strategy is designed in part to offset advantages in Allied air power, and thus gain strategic and tactical air superiority at a time and place of Moscow's choosing. Russia is also investing significant efforts in the development of autonomous weapons systems as part of a new force architecture. These include autonomous, robotic and remotely-controlled systems, new and advanced forms of electronic warfare (EW), as well as a rapidly-expanding offensive and defensive cyber capabilities. Russia's armed forces are also fast developing advanced command and control systems designed to exert effective and sensitive political control at the strategic apex of force, whilst at the same time developing a better devolved command authority culture on the battlefield. The Russians are also steadily increasing their already extensive use of battlefield internet, as well as enhanced ultra-range air defence and missile defence systems, and burgeoning anti-satellite (ASAT) capabilities that threaten NATO SIGINT and milsatcom architectures.

The focus on air power is also driving Russian advances in the development of '5G' fighters. The aim is to (at least) match Allied aircraft, such as the *F22 Raptor* and *F35 Lightning II*, and threaten them with advanced air defence systems, such as the S-400, and from 2020 the S-500 (*Prometheus*) system. Russia is enhancing the battlefield mobility of its forces, and seeking to make deployed Russian forces far more robust than in the past. However, it is the Russian interest in the development of hyper weapons and directed energy weapons which should be of great concern to Allied planners. Specifically, Moscow is developing so-called hyper-sonic weapons, as well as a new and robust generation of nuclear warheads, as part of a next-generation intercontinental ballistic missile system that would be effectively impregnable against future Allied missile defences. The new architecture Moscow is seeking to develop could also be capable at some point of remote command via artificial intelligence systems, and autonomous 'learning' systems.

[7] "Russian Military Doctrine article by General Valery Gerasimov", rough translation by Robert Coalson, June 2014 https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597

US future war military technologies include autonomous systems, unmanned undersea vehicles, advanced sea-mines, hyper-sonic strike weapons, advanced aeronautics, and new weapons systems such as electromagnetic rail-guns, and high-energy lasers. The US *Long-Range Research and Development Planning Program* includes military robotics systems, system autonomy, weapons miniaturisation, scaling big data for applied military use, artificial intelligence and deep-learning, all as part of new military-strategic concepts. The Pentagon is also seeking to establish innovative relationships with US industry so as to deploy the technologies and intellect across the US national supply chain (not simply the defence supply chain) in support of the defence effort. This kind of civ-mil-tech interface goes far beyond such relationships in Europe, and there is clear evidence China and Russia are following a similar track.[8]

The US is also developing new and advanced nuclear and space-based capabilities, advanced sensors, extreme range stand-off weapons, and communication systems designed for twenty-first century warfare. Most European allies are either failing to invest at all in such futures, or investing at levels far below the US, China and Russia. Moreover, Beijing, Moscow and Washington are all looking to develop more advanced missile defence systems, as well as extensive offensive and defensive cyber capabilities.

Russia's Future War Aims

On 1 July, 2014 President Putin said, "In the past 20 years, our [Russia's] partners have been trying to convince Russia of their good intentions, their readiness to jointly develop strategic co-operation. However, at the same time they kept expanding NATO, extending the area under their military and political control ever closer to our border".[9]

The replacement of 'right' with 'might', and the rejection of the community concept of international relations central to the idea of the European Union, is part of an 'eternal' search by Moscow for a new Russia-friendly balance of power in Europe. As such, Moscow's strategy embraces several strategic ends, the most notable of which is the re-drawing of the post-Cold War European strategic map, via the effective expulsion of the United States from Europe and by keeping other European powers divided and/or permanently strategically and politically off-balance.

To better understand the Russian view of future war, and the interaction between technology and strategy across the hybrid, cyber, hyper spectrum, it is useful to look at Russian strategy as a case study. Napoleon once said that "The art of war does not need complicated manoeuvre…The most difficult thing is to guess the enemy's plan, to find the truth from all reports. The rest merely requires common sense…"[10] Russia's future war strategy is a function of a grand strategy that reflects President Putin's anti-western world-view, allied to a sophisticated understanding of the West's many divisions and vulnerabilities, and how best to exploit them. Russian strategy is now part of a single-minded effort to do just that. The centralisation of power on the President's Office, and indeed on his own person, intensifies and reinforces the policy assumptions that underpin it. What is perhaps different from the past is that Moscow has learnt to exercise power in a more nuanced manner than the Soviet Union, or Tsarist Russia before it.

Russia's strategic aim is to create a buffer zone to its south and west, and to gain control over its high north, including the Arctic Circle, and along the entirety of its northern border that will likely form the new Northeast Passage between Asia and Europe. Moscow would also like to

[8] The Russians seem to have embraced the important point made by General John R. Allen and Amir Hussain when they wrote, "If, indeed, we are poised at the edge of hyperwar, we must explore the changes necessary to adapt to this new conflict environment…Our adversaries and our enemies are moving forward aggressively in this area. The United States must make the strategic investments both to be ready to wage hyperwar, and to prevent us from being surprised by it". See Allen, J. & Husain A. (2017) "On Hyperwar", in "Proceedings", July 2017, (Washington: US Naval Institute) p 27.

[9] "Conference of Russian Ambassadors and permanent representatives", Moscow, 1 July, 2014. See http://en.kremlin.ru/events/president/news/46131

[10] Cornwell, Bernard (2015) "Waterloo; The History of Four Days, Three Armies and Three Battles" (London: Harper)

weaken transatlantic ties to force some European states into a Russian sphere of influence, and compel the rest to comply with Russian strategic interests. In an 'ideal' Kremlin world, Russia's Future War Strategy would thus see the eventual expulsion of the US, Canada, and even the UK from Europe and its institutions, and the creation of a new Russia-friendly European security 'architecture'.

Russian strategy has been described as non-linear warfare. This is an entirely inadequate description of Russian strategy. Rather, Moscow is applying strategic deception (*Strategic Maskirovka*) as grand strategy. In essence, *Strategic Maskirovka* is a form of high or grand asymmetric warfare by a relatively weak, but nevertheless unitary actor, against an ostensibly far more powerful, but also more pluralistic, fractured group of actors at a moment of their maximum vulnerability.

The aim of Russian strategy is the preservation of the Putin regime. To that end, Moscow is deliberately creating tensions with the West to present Russia as a victim, in order for the Kremlin to reinforce its authority domestically in spite of the excessive security burden the Kremlin places on Russian society and economy. As such, the Putin regime is utterly cynical when it comes to its understanding and use of power, and in its appreciation of Russia's strengths and weaknesses.

The nationalistic exploitation of expansionist Russian history is a key element in the Kremlin's strategy. Indeed, President Putin and his regime have a romantic, uniquely Russian nationalist view of history, informed by past heroes such as Alexander Nevsky and Peter the Great, about Russia's place in the world, reinforced by the 1941-1945 Great Patriotic War against 'fascism'. It is a view furthered by President Putin's own prejudice about and against the West, and what he believes are past hurts the West inflicted on Russia. Consequently, NATO is vilified as an extension of traditional Western aggression towards 'peace-loving Mother Russia'. These efforts are reinforced by the promotion of a personality cult around President Putin that presents him as Russia's 'super-patriot'.

For all the bellicose rhetoric and aggressive military posturing Russia still does not want war. As Professor Michael Clarke has observed, "In a disordered world the powerful live with an existential threat of war that may be remote but which affects them in a number of more immediate ways. It is remote in that the prospect of war directly between the powerful states themselves is now hard to imagine. The ruinous costs of major wars, the shrivelled political advantage they would be likely to give the victor, the sheer unpredictability of the consequences, all indicate that war between them is highly unlikely".[11] Rather, Moscow is using the threat of both a limited, and/or a more general war, to sow division between the US and its European allies and to force tacit acceptance of Russian territorial aggression, most notably in Ukraine, and Russian influence elsewhere.

Thus, Russian strategy must be seen as a whole-of-state, whole-of-conflict spectrum, regional dominance game designed to ensure Russia can exert effective control over a self-defined 'strategic neighbourhood' via strategic manipulation. The strategy rests on the threatened use of re-strengthened armed forces as both a strategic lever and the ultimate arbiter in any conflict. This strategy is allied to a narrative that exaggerates Russian strength, but which masks Russia's many inherent, and potentially debilitating, weaknesses. The cost of such a strategy is high, but it has been strengthened domestically through the destruction of independent civil society and other sources of potential opposition to the Putin regime, and further reinforced by the centralisation of all state organs of power, with security, defence and intelligence structures re-established at the very core of the state and its identity. The danger of such closed systems is that policy assumptions become self-fulfilling, and thus prone to miscalculation, hubris, or both.

[11] See Clarke, Michael, (2012) "Does War Have a Future?" in Lindley-French J. & Boyer Y. (ed.) "The Oxford Handbook of War" (Oxford: Oxford University Press) p. 653.

The desired outcomes the Kremlin seeks would be Russian-friendly trade-offs as part of a transactional military and economic relationship with the rest of Europe, in which Moscow has the whip hand. The strategy presumes limited cooperation combined with the threat of confrontation, even nuclear confrontation, allied to offers of energy 'security' if European powers exclusively import Russian oil and gas.

Russia is not alone in seeking a return to a more classical balance of power. Indeed, *Strategic Maskirovka* is part of a growing use of strategic asymmetry by illiberal regimes across the world, to dismantle the rules-based system of international relations the West built. This is partly because such powers do not believe that the Western system of 'right' serves their respective interests, and partly because President Putin, and to lesser extent President Xi of China, believe that such a system is simply a control mechanism or device by and for the US and the wider West. President Putin firmly believes that over the past twenty of so years the West itself abandoned the rules-based system it created, when it served Western strategic convenience.

Russia's Future War Strategy

Russian future war strategy is purposeful and combines the threat of all force with disinformation and de-stabilisation from the very top of the state, through tightly-controlled multiple messaging, to the possible application of force at several levels of escalation intensity. President Putin is the architect of this strategy, a new/old Russian strategic method that can be summed up as the conduct of war via 5Ds: de-stabilisation, disinformation, strategic deception, disruption, and, if needs be, destruction. Russia's close analysis of European societies and political elites has convinced the Kremlin that many European states no longer possess the political will to deter Russia, or run the political risk all credible deterrence demands. As such Moscow believes many Europeans are particularly prone to wishful thinking about Russian policy and strategy, namely that Moscow too wants friendly relations. Consequently, Moscow believes European elites and peoples are susceptible to political manipulation underpinned by conflicting strategic messaging, much of it from President Putin himself, allied to the threat of overwhelming, sudden force, that plays on European memories of World War Two, the Euro-strategic balance of the 1980s, and a renewed threat of mutually assured destruction (MAD).

Russia's future war preparedness combines the build-up of Russian nuclear and conventional forces on NATO's border, the destabilisation and intimidation of states around all of Russia's northern, western and south-western borders, the intimidation of EU and NATO allies, and routine offers of 'peace' in return for a Russian veto over NATO policy. Moscow backs up such efforts with political agitation to suggest Russia's enforced indispensability to European/Western 'strategy', and thus influence over it. This approach has been particularly evident in Moscow's support for the Assad regime and its highly-conditional anti-ISIS co-operation with the US and its allies and partners. Russian involvement in the Middle East has little to do with the region, but everything to do with Europe and Russia's influence therein. Future historians may well propose that, even insofar as the Syrian civil war was a policy catastrophe for the US and the West more broadly, Russian support of the Assad regime and its complicity with the genocide in Syria actually served the greater strategic Russian purpose of destabilising European society and polarising its politics, by virtue of the near constant flow of Syrian and regional refugees into Europe; a flow abetted by the Russian incursion into the conflict and active support for the regime's horrendous attacks on its own population.

However, for all of its undoubted sophistication, Russian future war strategy must still balance capability with affordability. That is why Moscow's military doctrine goes far beyond the armed forces and rewrites ideas about the utility of force to combine hybrid warfare, cyber warfare, 'conventional' warfare, warfighting nuclear warfare, and hyper warfare into a future war meme that bestrides the strategic and the tactical. Strategic deception is central to that strategy with *Strategic Maskirovka* an adaptation of Russia's traditional use of battlefield deception, which is why in 2016 Russia invested some $250m in offensive cyber capabilities alone.[12]

Russia's future war strategy is, in effect, war at the many seams of the West, and acts across the conflict spectrum from disinformation to disruption to destruction. At the lower end, Russian strategy employs electronic means, use of propaganda (fake news), and FSB (Russian foreign intelligence services) interference in the electoral processes of the Western democracies to cause as much internal division and dissent as possible. Moscow understands that effective security and defence policy in any state rests necessarily upon a significant level of social cohesion and support. With Western European states now divided into many groups, ideologies and belief-systems, Moscow believes it can successfully undermine their respective security and defence policies. This approach is reinforced by consistent messaging to reinforce the belief in Europe that 'Russia is back', a superpower re-born, even though that is very far from reality.

Russia's Future War Structure and Method

On 26 June, 2014 President Putin signed, "On Strategic Planning in the Russian Federation", which instructed all social, economic and political development to be linked and considered within the framework of national security. At the centre of the planning concept is a new National Security Strategy and Plan for Defence. This follows a June 2013 order that gave the General Staff powers to co-ordinate the work of all federal agencies with executive power in "securing national security and defence".

To conduct such a strategy, the Russian state under Putin has been re-organised along Soviet-lite lines. In September 2009 President Putin issued a Presidential Order (Ukaz) requiring the linking of all situation centres and ordering the creation of a new inter-agency information sharing system. A new National Defence Management Centre (NDMC) was ordered by a Presidential 'Ukaz' (decree) on 10 December, 2013, following the bungled August 2008 military operations in Georgia, and after lessons had been identified and learned. On 20 January, 2015 Defence Minister Shoigu likened the then-new Centre to the re-creation of the old Stavka of the Supreme Commander of Soviet Forces. Whilst still very much a work in progress the NDMC is at the very heart of Russia's future war strategy and covers the spectrum of strategies, campaign and operations from hybrid war to hyper war via cyber war. The NDMC became operational on 1 December, 2014, with its given purpose to link all departmental systems concerned with the management of monitoring of 'defence' (offensive and defensive), and to act as national information hub and headquarters, including a strong civil-military component to promote a cohesive whole-of-government approach. This whole-of-government approach has been further reinforced by the planned re-creation of another Soviet-era organ, a new pan-government mega-ministry called the Ministry of State Security (MGB).

At the military-strategic level, Russia is seeking to exploit growing American military over-stretch to 'demonstrate' to Europeans the growing incapacity of the US, and be extension the inability of NATO to defend them. Russian intent is reinforced by 'proving' Moscow's growing mastery of coercive military power via snap exercises, blue water deployments, aggressive nuclear posturing, reinforced A2/AD capabilities, and leadership of new thinking in warfare – future war.

Russia's future war strategy is also being steadily operationalised. In June 2015 General Vladimir Zarudnitskii, Chief of the Main Operational Directorate of General Staff said: "The creation of the National Defence Management Centre (NDMC)…will make possible the creation of a system covering all links of the leadership of the armed forces and also give the

[12] "NASA CI/CT Monthly News Update – March 2016". https://www.hq.nasa.gov/office/pao/FOIA/newsletters/CI-CTNewsletter_March_2016_TAGGED_Redacted.pdf

possibility in an operational regime to co-ordinate the efforts of 49 ministries and government departments participating in the fulfilment of the Plan of Defence of the country".[13]

The NDMC includes the Federal Strategy Centre, situation centres, information and stratcom command and control, with a direct link to the President's Office. It also affords President Putin real time strategic options and intelligence, with real time assessment of Russian forces and resources, including the readiness of military districts, the role, state and preparedness of the other 'power' ministries (home, foreign, MGB), as well as non-military aspects of Russian strategy. Crucially, NDMC also monitors the strategy and armed forces of foreign states, as well as the world-wide media. In addition to its functions as a campaign hub the NDMC also includes: the Centre for the Management of Strategic Nuclear Forces; the Centre for Combat Management; the Centre for Daily Management of the Armed Forces. To ensure its writ runs far beyond Moscow the Centre has offices in the HQ of each Oblast or military district.

Future War NATO?

Bernard Brodie once said that, "Deterrence is a strategy designed to dissuade an adversary from an action not yet taken".[14] NATO Adaptation must necessarily be a first step towards a future war Alliance deterrence and defence posture. How far is NATO towards crafting a sound future war strategy? Only a NATO that demonstrates unequivocally that it is adapting to future war will ensure and assure the deterrence and defence required to prevent it. Future war will thus require the Alliance to deter an 'adversary' by having the capacity – both directly and indirectly – to take many actions at many levels of conflict, across the conflict spectrum, and often simultaneously.

Several decisions taken at the 2014 Wales Summit and the 2016 Warsaw Summit suggest that the Alliance is at least moving in the right direction as it begins to grapple with the implications of future war. However, such efforts are as yet insufficiently ambitious, holistic, and/or properly resourced to be called a NATO Future War Strategy – the outcomes-driven test of NATO Adaptation.

The Defence Investment Pledge to spend a minimum 2% GDP on defence by 2024, of which 20% per annum must be spent on new equipment, is an important statement of intent. And yet, several NATO nations are already questioning that solemnly agreed goal, or trying to circumvent its meaning by challenging how such expenditures should be calculated, and what expenditures such be included. Worse, the overwhelming focus of most of the Allies on domestic expenditures, including defence budgets, is in danger of fatally weakening the collective authority each Ally gains through NATO, and upon which the credibility of their own respective security and defence rests. The Readiness Action Plan and the Enhanced Forward Presence are also important commitments to deterrence, but only as far as they go, some consider them 'trip wire' forces at best. Russian forces far outnumber their Alliance counterparts on NATO's eastern flank, and seem to be held at a higher state of readiness, which was demonstrated by the September *Zapad (West) 2017* exercise.

Between 14 and 20 September, 2017 Russia, and its junior partner Belarus, (the so-called 'Union State') conducted the largest military exercise in Europe since the Cold War. The exercise took place centred on Brest close to the Belarussian border with Poland, as well as in Kaliningrad, the small Russian enclave some 60 kilometres from Belarus across NATO territory. *Zapad 2017* incorporated a massive series of wargames involving between 60,000 and 100,000 military and civilian personnel. Crucially, the exercise tested Russian military and civilian readiness and effectiveness across a conflict spectrum that stretched from hybrid warfare to hyper warfare via cyber warfare, backed up by the threat of nuclear force and strengthening anti-air, area defence (A2/AD) capabilities – the new linear/non-linear order of twenty-first century strategic battle pioneered by General Gerasimov.

[13] Lindley-French J. (2015) "Countering Strategic Maskirovka", (Ottawa: CDFAI).

[14] See Chambers, J.W. & Anderson J. (1999) "The Oxford Companion to American Military History" (Oxford: Oxford University Press) p. 215

NATO? Continuing reforms of the NATO Command Structure are indeed underway, allied to ongoing efforts to improve military interoperability via a range of initiatives, such as the 16 nation Framework Nation concept, and the Transatlantic Capability Enhancement and Training Initiative (TACET). All such efforts suggest the military and intellectual underpinnings needed for a NATO Future War Strategy are beginning to fall into place, in no small part due to American prompting and the funding provided by the European Reassurance Initiative.

A truly sound and credible NATO Future War Strategy would need to be far more holistic, far more joined up, and far more ambitious, and demonstrably match an adversary across the hybrid-cyber-hyper strategic continuum. The Alliance needs to go far further and far faster if a credible NATO Future War Strategy is to be established that could underpin a future Alliance deterrence and defence posture, reinforced by forces able to sustain a high level of readiness, responsiveness, and resilience across the conflict spectrum. NATO Force Structure reform, the Joint Expeditionary Force (JEF), the Cyber Defence Pledge, NATO Baseline Requirements for National Resilience, heightened interoperability, the Alliance Maritime Posture, institutional adaptation, and efforts to modernise platforms and systems development with industry are all well and good. However, they are insufficiently embedded in the respective national strategies of Allies, with progress too often measured by limited, marginal improvements to existing structures, and undermined by weak links to the civil intellectual and industrial resources which, in many ways, are driving the strategy and technology underpinning future war, albeit often unwittingly.

Future deterrence also rests upon strong resilience and manifest systemic redundancies in enablers, systems and infrastructures. At its most simple, the Alliance and its nations will need the capacity to block mass fake ‘strategic’ messaging, and to beat an adversary to a message. This in turn will require an effective counter-hybrid warfare strategy built on agile and resilient strategic communications. Alliance societies also need to be become far more hardened against terrorism, attacks on critical infrastructures, and denial of critical services so that consequence management and recovery also become demonstrably more agile. Critically, NATO must be able to undertake offensive and defensive cyber operations to deny an adversary the ‘free’ cyber-space to undertake attacks against the Alliance and its peoples. Above all, adapted twenty-first century deterrence will need Allied forces armed with the systems, platforms, and structures at the very cutting edge of technologies able to overcome an adversary, most notably in the area of anti-access, area-denial (A2/AD). A2/AD is increasingly expanding beyond point defence or limited area defence, to the defence of growing strategic ‘space’.

Much like Russia’s future war strategy, the Alliance strategy will necessarily be as much about structure and organisation, as technology will also require the Alliance to craft an integrated deterrence concept that also promotes functional cross-government civil-military co-operation. In Europe, which will remain the main theatre of NATO operations, such a strategy will thus mean a new form of civil defence and a conscious effort to prove to an adversary an innovative edge and critical comparative systems advantage. This aim will place particular importance on real ‘strategic partnerships’ with other institutions, most notably the European Union.

Responsiveness, readiness, agility and adaptation will thus go hand-in-hand in defeating a future war adversary that seeks to use mass disruption and mass destruction in dark tandem. Critically, given the accelerated pace of destruction in a future war, the NATO Secretary-General may well need to become akin to a strategic chief executive officer with far more devolved authority from the North Atlantic Council than at present. Simply reacting may simply be too slow (and too late) especially with the looming prospects of hyper-war. SACEUR and his/her team will also need to be far more empowered to be nimble and agile, particularly at the strategy/intelligence/political/capability interface, and far more empowered to use his/her individual judgement in every sense. Indeed, the lack of established and practiced command agility is one of the most profound weaknesses from which the Alliance suffers. The full exploitation of new NATO capabilities in hyper warfare thus demands a corresponding agility in the decision-making processes, so that they are better, faster, and more reliable and resilient than any enemy. Otherwise, the capability advantage would be at best compromised, at worst dangerously diminished.

Consequently, to deter future war, NATO will need a measured future war strategy of its own, built on a firm foundation of understanding about the nature, extent, and above all, the immediacy of threats and their strategic and tactical interplay. At the very least, NATO will need the twenty-first century equivalent of Wellington's 'Exploring Officers', part of which will necessarily include a new and deeper partnership between academia and intelligence to better understand Russian (and other) intentions, capabilities and actions. Countering future war will also require far more intense, and far deeper co-operation, between military and criminal intelligence to better prevent penetration of Western societies and to counter Russia's ability to wage war at the seams of Western societies, thus preserving the vital balance between protection of people and projection of force. Or, to put it another way, future war will demand of NATO and military establishments new cultures and new ways of doing business, often with people who in the past have not been either natural or easy partners.

NATO's Future War Strategic Concept

If NATO is to match Russia it must also demonstrate improved military resolve, responsiveness and readiness. A credible NATO Future War Strategic Concept must thus be the outcome of NATO Adaptation which, at the very minimum, must see the Alliance redefine full spectrum warfare, and its role therein. Such a Concept would help drive forward the hardening of systems and structures upon which all Alliance society depends to function. Crucially, this new Strategic Concept ("From Hybrid War to Hyper War via Cyber War") would demonstrate to the world an Alliance not only adapting to twenty-first century warfare, but able to deter it, and if needs be fight it.

The Concept would be a far more applied document than its 2010 forebear, and help drive the future war security and defence choices and investments of all the Allies. It would necessarily include an Alliance stratcom and information warfare strategy to counter Russia's use of *Maskirovka*, a resilience strategy to help shore up both the seams between government and society, identify 'strategic infrastructures' vital to the defence of the Alliance, and an adapted nuclear policy that communicates credibly there would be an overwhelming NATO nuclear response should any such weapons be used against the Alliance, however low the yield. NATO cannot permit the delusion to be held anywhere that such weapons have a warfighting role, or could be used for nuclear blackmail. Critically, the Concept would also need to demonstrate the determination of the Alliance to overcome any perceived 'deterrence gap' that may emerge because of exotic technologies, most notably in the area of offensive cyber capabilities.

A NATO Strategic Concept would also enshrine an outcomes-driven NATO Strategy for Future War at its core. The future Alliance military posture would also need to be front and centre of the new NATO Strategic Concept. Future War will demand that NATO develop a kind of strategic defence 'singularity' – THE future war command hub for the Allies and partners. Even before a New Strategic Concept is agreed, specific, immediate steps should be taken now (and which will cost little in the short-term), which could include (inter alia);

- realistic exercises that, again, involve political leaders to promote elite political cohesion
- the further establishment of NATO at the core of a matrix of stabilising and legitimising institutions
- the sharpening of intelligence and early-warning systems
- the hardening of strategic military communications

- force adaptation to better engage across the emerging conflict spectrum, including the exploitation of new technologies
- development of future war programmes of education for civilian and military leadership
- enhancement of expertise via innovative mil-mil and civ-mil exercises

There will, of course, be a cost to establish credible NATO Future War readiness, but it need not be prohibitive. Structurally all of the above begs better EU-NATO co-operation and should be central to a future EU-NATO Strategic Partnership.

For all the organisational and structural steps NATO needs to undertake, defence innovation is ultimately the key to future war. Sadly, Europeans are far behind the US in investing in the new technologies and sciences that will drive and define the character of war and conflict in the twenty-first century.[15] For that reason it would be useful for the Alliance to stand up an organisation similar in ambition to the US *Defence Advanced Projects Research Agency* (DARPA) with which it could partner. Only via such a radical approach will the Alliance be able to shift to the outcomes-led strategy future war will demand of it.

A truly reformed NATO Defence Planning Process (NDPP) would have a vital role to play in establishing the basis for rational defence choices by all the Allies given the future war challenge. At the very least, the NDPP must be placed far more to the fore of the defence planning of all the Allies, effectively driving force and equipment planning choices. Indeed, a future war NDPP will be vital if the Alliance is to meet the core threat – the future force-on-force challenge.

Scenario 2:

Strat-Tech War 2025 - NATO Victory in the Second Battle of North Cape

It is August 2025. The United States is mired in growing short-of-war, but nevertheless dangerous conflicts in Asia-Pacific. Europe is vulnerable, exhausted and worn down by years of hyper-migration from its south, Brexit, a seemingly endless flow of terrorist attacks, and years of relative economic decline caused by leaders unable or unwilling to take the necessary measures to resolve Europe's myriad political, economic and social tensions.

In July, Russia moved a large formation of Naval Infantry (marines) to Pechenga, close to Russia's short border with Norway. Alarmed Oslo called for Alliance support. As tensions increase, and by way of response, on August 10th, the North Atlantic Council ordered SACEUR to take all necessary steps to demonstrate to Moscow the Alliance's determination to defend its borders.

A NATO Task Group, that has been working up to full operating capability for some years is despatched by SACEUR to demonstrate intent. The Task Group is organised around the British heavy aircraft carrier and command ship *HMS Queen Elizabeth*, and include ships, aircraft and submarines from Britain, Canada, France, Germany, the Netherlands, and Norway. Critically, the Task Group is supported by the *Zumwalt*-class 'stealth' destroyer, *USS Lyndon B. Johnson,* acting as a form of 'picket ship' some way from the fleet, NATO Global Hawk maritime surveillance systems capable of monitoring threats operating across the bandwidth spectrum, together with P8 Maritime Patrol Aircraft armed with an array of intelligent anti-submarine systems, offer a further layer of deployed force protection. Under the fleet, two Royal Navy *Astute*-class nuclear attack submarines lurk. *HMS Ambush* and *HMS Audacious* can operate both as part of the Task Group they protect, or independently of it. On this

[15] Relative European weakness in field of defence innovation are acknowledged by Europeans themselves. An influential 2016 report states, "…Europe's ongoing economic and fiscal crisis has clearly had a negative impact on the resources available to EU member-states to engage in security-related activities. At the same time, threats have become more 'hybrid', less conventional, and very difficult to tackle with traditional means and without international co-operation". See Group of Personalities (2016) "European Defence Research: The case for an EU-funded defence R&T programme" (Paris: EUISS) p. 19

occasion the two submarines are also acting as platforms and command nodes for fully-automated ‘defence bots’.

0430 hours, August 15th: The Second Battle of North Cape commences. Weapons and defence systems on board *HMS Queen Elizabeth,* driven by a range of artificial intelligence packages, suddenly surge into life, as the Russians try and fail to breach the cyber-defences of the Task Group.

0431 hours: An autonomous Russian underwater stealth platform launches a swarm of intelligent autonomous, flying armed ‘attack-bots’. Immediately, the NATO Task Group puts up an automated layered defence, and launches a counter-swarm of ‘defence-bots’, reinforced by the latest missile and ‘goalkeeper’ defence systems.

0432 hours: The commodore in charge of the Task Group orders the fleet to engage full, automatic defence. Interlocking systems on board all the ships engage the enemy, creating a ‘defence sphere’ around the fleet, on, above and below the water. Autonomous underwater bots begin to systematically search for the source of the Russian attack.

0433 hours: Using ‘block sonar/radar technology’ that creates a hi-def 3D picture above and below the fleet, two Russian *Yasen*-class nuclear attack submarines are identified, together with a *Sevastopol*-class unmanned underwater launch platform.

0434 hours: The now autonomous Task Group launches a wave of intelligent bots, the twenty-first century descendants of World War Two torpedoes and depth charges. Several ‘pods’ are launched from the two *Astute*-class nuclear attack submarines.

0434 hours: *HMS Queen Elizabeth* scrambles 809 Naval Air Squadron and its F-35B Lightning II/5 (ER) fighters to provide top cover against any possible Russian manned air incursion. She also deploys EH-101 Merlin 7 helicopters, together with a host of data-link and weapons drones. In fact, the manned systems are little more than back-up for increasingly sophisticated, long-range autonomous systems, a further layer of defensive redundancy just in case.

0437 hours: Three enormous underwater explosions are registered to the north and west of the Task Group. All a now-shocked and alarmed Moscow hears is silence…as *HMS Queen Elizabeth* and her NATO fleet forge forward. Deterrence achieved, collective defence confirmed.

0630 hours: After Russian losses are confirmed, a shocked President Putin picks up the telephone to the White House and several European leaders. He apologises to them all for what he calls “rogue elements within the Russian Navy” and the wholly unauthorised attack on the NATO force. He promises to do all in his power to root out the “traitors”.

Europe slumbers on, none the wiser…

From Hybrid War to Hyper War via Cyber War

Future war – from hybrid war to hyper war via cyber war - is the new way of war, not in the future, but now. This paper began with a scenario in which an under-prepared and under-equipped NATO force was quickly defeated by a more advanced and determined Russian force using the latest future war technologies. The paper concludes with an entirely different scenario in which the same battle is fought, but this time by NATO forces forged in preparation for future war, and which quickly and decisively defeats the aggressor. Either scenario is plausible. However, which scenario becomes more likely depends on decisions that need to be taken by Alliance political leaders, and taken now. The challenge? A truly adapted NATO must be a future war NATO.

NATO's new Future War Strategic Concept must realise an Alliance that has at its immediate disposal credible, intelligent, hard power and real smart power across the conflict spectrum. That will demand the modernisation of Article 5 to include rapid action, cyber-defence/offence, and hybrid defence/offence, and bespoke hyper war capabilities allied to a new concept of the very meaning of the word 'attack'. Only with Future Defence combinations will the Alliance be able to properly understand when the Alliance and its peoples are under threat, and if needs be successfully fight a future war.

If Adaptation is to be worth a row of beans the Alliance must be able and willing to meet the future war force-on-force challenge, from whomsoever and wherever it comes. Future war is one of THE real twenty-first century strategic challenges to the Alliance. Is NATO up to that challenge?

John R. Allen, Philip M. Breedlove, Julian Lindley-French & George Zambellas

About the Authors

General John Allen USMC (Retd.) is Senior Fellow of the Brookings Institution in Washington DC, the former Special Presidential Envoy for the Global Coalition to Counter ISIL, and former Commander of the NATO International Security Assistance Force in Afghanistan.

General Philip M. Breedlove (Retd.) is the former NATO Supreme Allied Commander, Europe (SACEUR) and Distinguished Professor at the Sam Nunn School at Georgia Tech.

Professor Dr Julian Lindley-French is Senior Fellow of the Institute for Statecraft in London, Director of Europa Analytica in the Netherlands, Distinguished Visiting Research Fellow at the National Defense University, Washington DC, and a Fellow of the Canadian Global Affairs Institute.

Admiral (Ret.d) Sir George Zambellas is the former First Sea Lord, Head of the Royal Navy.

Supporting Documents and Papers

Allen, J. & Husain A. (2017) “On Hyperwar”, in “Proceedings”, July 2017, (Washington: US Naval Institute)

Chambers, J.W. & Anderson J. (1999) “The Oxford Companion to American Military History” (Oxford: Oxford University Press)

Coker, C. (2015) “Future War” (London: Polity)

Cornish P. & Donaldson K. (2017) “World of War 2020” (London: Hodder & Stoughton)

Freedman, L. (2013) “Strategy: A History” (Oxford: Oxford University Press)

Group of Personalities (2016) “European Defence Research: The case for an EU-funded defence R&T programme” (Paris: EUISS)

Konstam, A. (2009), “The Battle of North Cape: The Death Ride of the *Scharnhorst*, 1943”. (Barnsley: Pen and Sword)

Lindley-French J. & Boyer Y. (ed.) “The Oxford Handbook of War” (Oxford: Oxford University Press)

Lindley-French J. (2015) “NATO: The Enduring Alliance”. (London: Routledge)

Lindley-French J. (2015) “NATO: Countering Strategic Maskirovka”, (Calgary: CDFAI)

Persson G. (2017) a critique of “The War of the Future: A Conceptual Framework and Practical Conclusions: Essays on Strategic Thought” by Igor Popov and Musa Khamzatov, (Rome: NATO Defence College)

Shirreff, Richard (2016) “2017: War with Russia”, (London: Coronet)

rj

GLOBSEC

Klariska 14
81103 Bratislava
Slovak Republic
Phone/Fax: +421 2 5441 06 09
info@globsec.org

www.globsec.org